Министерство образования и науки Российской Федерации

Московский Государственный Технический Университет
им. Н.Э. Баумана

Факультет «Информатика и системы управления»
Кафедра «Компьютерные системы и сети»

Сурков Л.В.

Методические указания
к лабораторной работе по курсу
Корпоративные сети

Раздел
Построение защищенных сетей с использованием брандмауэров

Протокол туннелирования PPPoE

2011

Протокол туннелирования PPPoE

Теоретические основы

Протокол PPPoE (Point-to-Point Protocol over Ethernet) применяется для подключения нескольких пользователей в одной Ethernet-подсети к удаленным пользователям другой Ethernet-подсети через общий последовательный интерфейс путем установления сеанса связи и инкапсуляции PPP-пакетов поверх Ethernet. Применяется как протокол туннелирования. Все пользователи сети делят одно подключение, однако контроль доступа может быть выполнен для каждого пользователя. Базовым протоколом PPPoE является протокол PPP.

Обзор PPP.

Протокол PPP был разработан для поддержки последовательных каналов типа «точка-точка». Протокол PPP описывается в стандартах RFC 1332/1661/2153, он инкапсулирует данные протокола сетевого уровня в данные канального уровня «точка-точка». Протокол PPP обеспечивает установку соединений между маршрутизаторами и подсоединение хоста к сети как по последовательным *синхронным*, так и по *асинхронным* каналам и , кроме того, обеспечивает возможность использования нескольких протоколов сетевого уровня (например, IP и IPX).
Протокол PPP использует три основных компонента.

- • Протокол HDLC (High-Level Data Link Control) используется в качестве основы при инкапсуляции дейтаграмм при передаче их по последовательным каналам типа "точка-точка".
- • Протокол LCP (протокол управления каналом) используется для установки и конфигурирования соединения, а так же для согласования и проверки кадров на канальном уровне.
- Семейство протоколов NCP (протоколы управления сетью) - для установки и конфигурирования различных протоколов сетевого уровня. Протоколы NCP обеспечивают возможность инкапсуляции различных протоколов сетевого уровня. Таким образом, протокол PPP поддерживает, кроме протокола IP, другие протоколы, в частности протокол IPX (Novell).

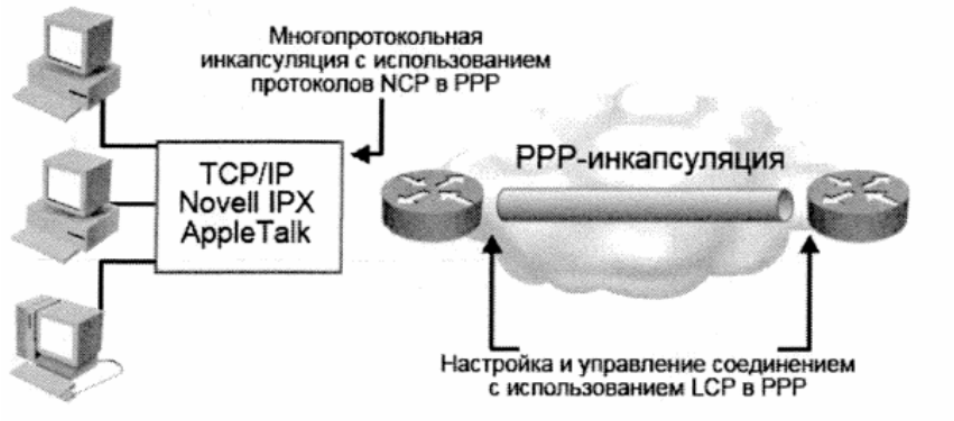


Рис. 1. Три компонента протокола PPP.

Установка сеанса связи в протоколе PPP

Протокол PPP предоставляет средства для установки, конфигурирования, поддержки и прекращения работы соединения "точка-точка", при этом последовательно выполняются следующие этапы.

1. *Создание канала и согласование конфигурации.* Первичный узел протокола PPP посылает LCP-фреймы для установки канала и согласования его параметров, таких как максимальный размер принимаемого блока, сжатие некоторых полей PPP или протокол аутентификации канала.
2. *Проверка качества работы канала* (необязательно). На этой стадии канал тестируется с целью выяснения, обеспечивает ли он достаточное качество для работы протоколов сетевого уровня.

Кроме того, после принятия решения о протоколе аутентификации можно проверить подлинность клиента или рабочей станции. PPP поддерживает два протокола аутентификации: PAP (вышел из употребления) и CHAP, оба описаны в спецификациях RFC 1334/1994.

3. К*онфигурирование протокола сетевого уровня.* Первичный узел протокола PPP рассылает NCP-фреймы, чтобы выбрать и настроить один или несколько протоколов сетевого уровня, таких как IP, Novell IPX. После настройки каждого из протоколов сетевого уровня датаграммы этого протокола можно передавать через канал.
4. *Инкапсуляция и передача* инкапсулированных дейтаграмм по последовательному каналу "точка-точка» по протоколу HDLC.
5. *Окончание работы канала.* Конфигурация канала связи сохраняется до тех пор, пока LCP- или NCP-фреймы не закроют канал, или до какого-либо внешнего события (например, истечения времени таймера простоя или вмешательства юзера).

Форматы фреймов протокола PPP

Фрейм протокола PPP состоит из следующих полей.

Размер поля в байтах	1	1	1	1	поле переменной длины	2 или 4
Назначение поля	поле флага	поле адреса	поле управления	поле протокола	поле данных	FCS

Рис.2. Формат PPP-фрейма

• *Флаг(1 байт).* Разделитель пакетов, указывает на начало или конец фрейма и представляет собой последовательность 01111110.
• *Адрес(1 байт).* Широковещательный адрес FF, указывает, что пакет адресован всем станциям.

Протокол PPP не назначает станциям индивидуальные адреса.

• *Управление(1 байт).* Один байт, содержащий последовательность 00000011, которая вызывает передачу данных, находящихся в неупорядоченном фрейме. При этом обеспечивается канальная связь без установки соединения, аналогичная связи протокола управления логическим каналом (Logical Link Control, LLC) первого типа.
• *Протокол.* Два байта, которые идентифицируют тип протокола, сформировавшего информацию в поле данных,например:

0021. Не сжатые IP-дейтаграммы.
002d. IP-дейтаграммы со сжатыми TCP- и IP-заголовками.
c021. Link Control Protocol (LCP).
c223. Challenge Handshake Authentification Protocol (CHAP).

• *Данные.* Содержат дейтаграмму протокола, указанного в поле протокола. Конец поля данных определяется байтом разделителя пакетов и выделения двух байтов для контрольной последовательности фрейма. По умолчанию максимальная длина поля данных равна 1500 байтов.
• *FCS (контрольная сумма).* Обычно состоит из 2 байтов, добавляемым к фрейму для обнаружения ошибок.

Протокол LCP (Link Control Protocol).

Используются три типа LCP-фреймов.
• *Фреймы установки канала связи.* Используются для создания и конфигурирования канала.
• *Фреймы поддержки работы канала.* Используются для отладки канала и для управления им.
• *Фреймы закрытия канала.* Используются для прекращения работы канала.

Протокол LCP применяется в PPP-соединениях для ведения переговоров о своих возможностях во время процесса установления соединения с целью достижения наиболее эффективного соединения. Сообщения протокола LCP переносятся фреймами протокола PPP и содержат информацию о возможной конфигурации соединения. Как только две стороны останавливаются на конфигурации, которую они обе могут поддерживать, процесс установления соединения продолжается.

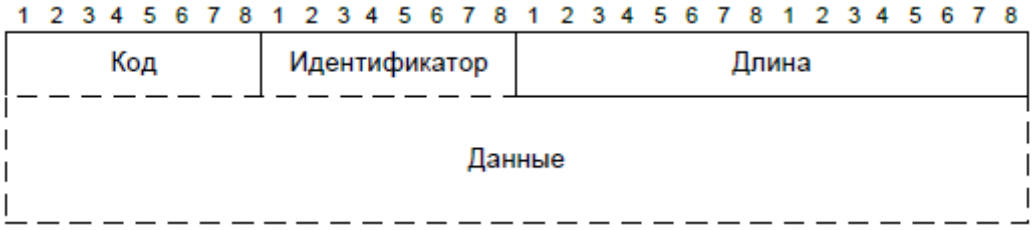


Рисунок 3. Формат LCP-фрейма

Функции полей LCP- фрейма следующие:
•. Код (1 байт) - определяет тип LCP-сообщения.
- 1 – Configure-Request.
- 2 – Configure-Ack.
- 3 – Configure-Nak.
- 4 – Configure-Reject.
- 5 – Terminate-Request.
- 6 – Terminate-Ack.
- 7 – Code Reject.
- 8 – Protocol Reject.
- 9 – Echo-Request.
- 10 – Echo-Reply.
- 11 – Discard-Request.

- Идентификатор (1 байт). Содержит код, используемый при ассоциации запросов и ответов на них для индивидуальной LCP-транзакции.
- Длина (2 байта). Определяет длину LCP-сообщения, включая все поля.
- Данные (переменный размер). Содержит элементы, состоящие из трех полей:

  тип (1 байт). Определяет конфигурируемую опцию, например:

  - 1 – максимально принимаемый блок.
  - 3 – протокол аутентификации.
  - 14 – время соединения.

  длина (1 байт). Определяет длину элемента, включая все поля.

  данные (переменный размер).

Протоколы аутентификации PAP/CHAP

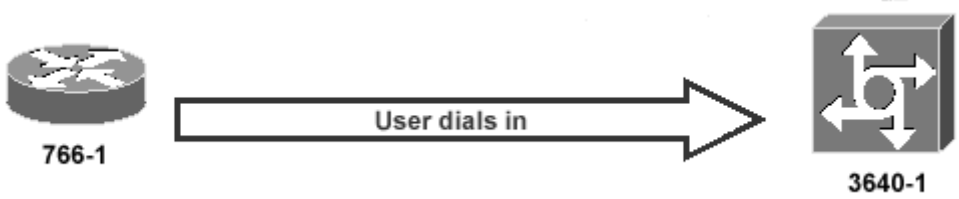
Этап аутентификации сеанса PPP не является обязательным.

Протокол PAP является слабым протоколом аутентификации, использует двухстороннее квитирование установление связи и передает логины и пароли открытым текстом.. Кроме того, отсутствует защита от повторного воспроизведения или повторных атак. Однако попытки подключения, их частота и время регистрируются удаленным хостом.

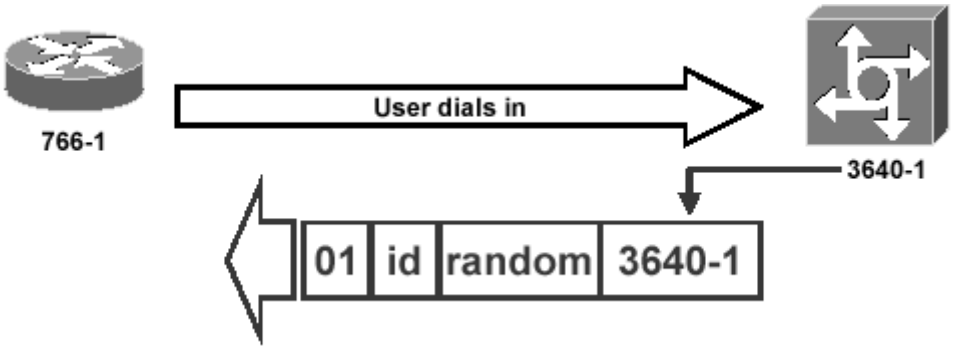
Предпочтительный протокол CHAP используется для зашифрованной периодической проверки подлинности удаленного узла с использованием метода трехэтапного квитирования (вызов – ответ - принять/отвергнуть). Такая проверка может быть повторена в любой момент времени, что делает его менее уязвимым перед попыткой хакеров проникнуть в сеть. Протокол CHAP обеспечивает защиту от атак повторного воспроизведения путем использования уникального и непредсказуемого значения сообщения вызова, которое, как правило, рассчитывается с помощью односторонней функции кэширования (обычно Message Digest 5, MD5). Частота и время отправки сообщений вызова определяется маршрутизатором или сервером аутентификации.

Рассмотрим подробнее процесс аутентификации соединения с помощью протокола CHAP.

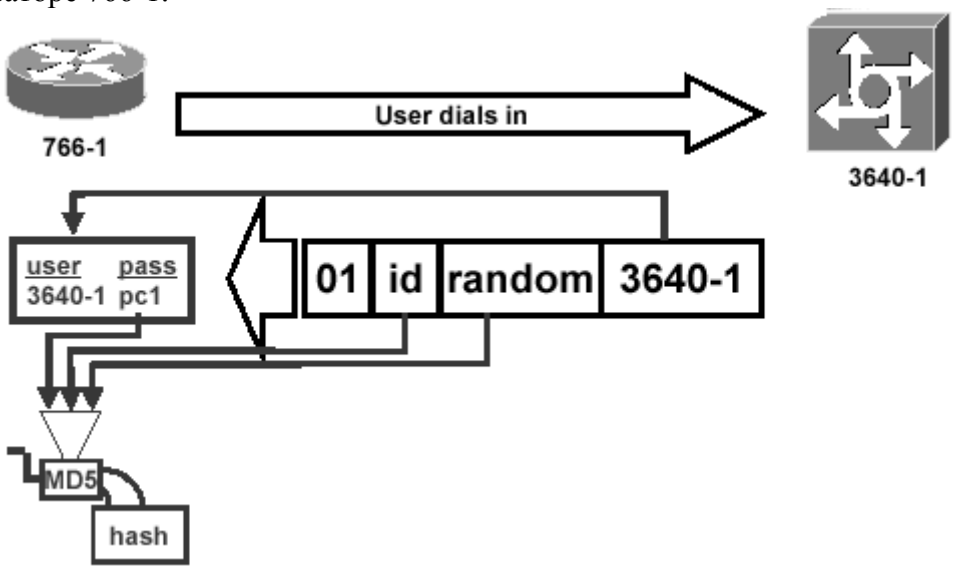
Этап 1. При попытке подключения удаленного пользователя (766-1), сначала осуществляется предварительная настройка соединения с помощью протокола LCP. При этом на входящем порте маршрутизатора, к которому осуществляется подключение (3640-1), должна быть включена аутентификация по протоколу CHAP.



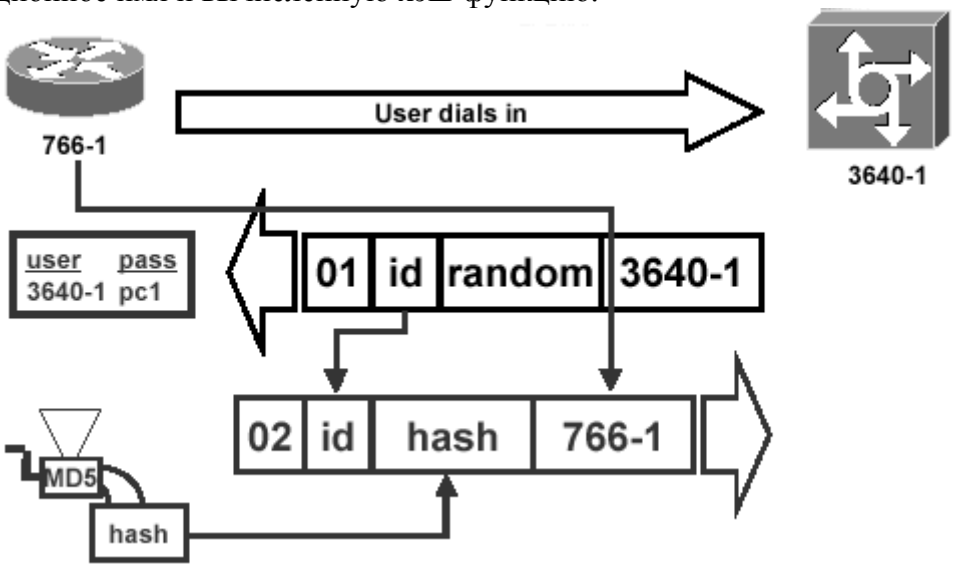
Этап 2. После предварительной настройки соединения вызываемая сторона (3640-1) посылает кадр-запрос для проверки подлинности абонента. В кадре содержатся следующие поля:
01 = тип кадра – кадр-запрос;
ID = порядковый номер, идентифицирующий запрос;
Random = произвольные числа, генерируемые маршрутизатором;
3640-1 = идентификационное имя источника запроса.
Значения полей ID и Random запоминаются в маршрутизаторе (3640-1).



Этап 3. Вызывающий абонент принимает кадр-запрос и обрабатывает его следующим образом: вычисляет хэш-функцию (алгоритм MD5) по содержимому полей кадра-запроса ID и Random, а также по паролю, соответствующему записи 3640-1 в локальном маршрутизаторе 766-1.

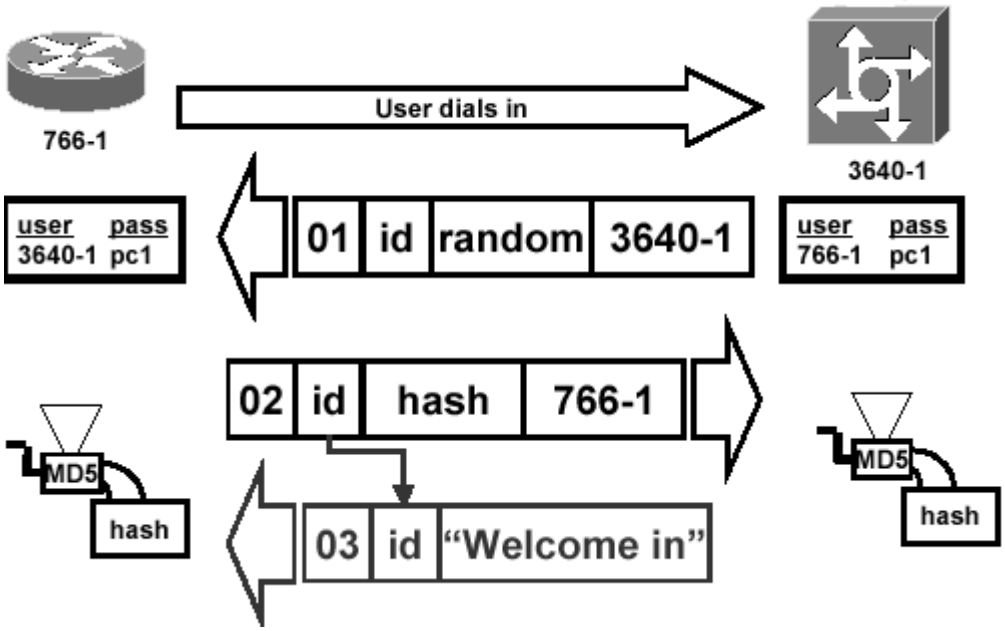


Этап 4. Абонент посылает сформированный кадр-ответ, содержащий его идентификационное имя и вычисленную хэш-функцию.



Этап 5. Маршрутизатор 3640-1 принимает кадр от абонента, вычисляет хэш-функцию, используя ту же самую информацию, и сравнивает с содержимым поля hash кадра-ответа от абонента. Если значения хэш-функций совпадают, то абоненту посылается

уведомление об успешной аутентификации. Иначе, посылается кадр, информирующий об отказе в соединении с абонентом. В первом случае в поле типа кадра будет содержаться значение 03, а во втором – 04. А в поле данных заносится простая текстовая строка, например, «Welcome In» или «Authentication failure».



Настройка параметров аутентификации

Чтобы включить инкапсуляцию PPP с аутентификацией PAP или CHAP на интерфейсе, выполните следующие действия:

Этап 1. Задайте имя хоста маршрутизатора в качестве его идентификатора

Router (config)# **hostname** имя

Этап 2. Задайте имя и пароль пользователя *удаленного* маршрутизатора

Router (config)# **username** имя **password** пароль

Этап 3. Войдите в режим установки конфигурации требуемого интерфейса.

Этап 4. Установите инкапсуляцию PPP в качестве протокола второго уровня на этом интерфейсе

Router(config-if)# **encapsulation ppp**

Этап 5. Выберите режим аутентификации PAP и/или CHAP

Router(config-if)# **ppp authentication {chap|chap pap|pap chap|pap}**

После того как параметры протокола PPP установлены, состояние его LCP и NCP может быть проверено командой **show interfaces**.

При вводе команды **ppp authentication chap pap** маршрутизатор попытается аутентифицировать все входящие сеансы PPP с помощью CHAP. Если удаленное устройство не поддерживает CHAP, маршрутизатор попытается аутентифицировать сеанс PPP с помощью PAP. Если удаленное устройство не поддерживает ни CHAP ни PAP, аутентификация считается неудачной и сеанс PPP отбрасывается.

Пример конфигурирования


```
hostname RouterX
username RouterY password sameone
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
```

```
hostname RouterY
username RouterX password sameone
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
 ppp authentication chap
```

Обзор PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) применяется как протокол туннелирования, используемый для подключения нескольких пользователей в одной Ethernet-подсети через общий последовательный интерфейс, например, кабельный модем, DSL-линия, беспроводной канал. PPPoE даёт провайдеру следующие преимущества:

- аутентификация по логину/паролю;
- автоматическое выделение IP-адресов пользователям (похоже на DHCP);
- автоматическое определение PPPoE-сервера.

Так как физически устанавливается PPP-сеанс связи, то PPPoE-соединение обладает всеми свойствами PPP-соединения. Процесс установления PPPoE-соединения состоит из 2 стадий:

- поиск PPPoE-сервера (Discovery);
- установление PPP-соединения.

На стадии поиска клиент производит поиск PPPoE-сервера. Если в сети используется несколько серверов, то происходит выбор одного из них. Так как PPPoE-соединение организуется на канальном уровне, то его установление между участниками соединения идет по MAC-адресам. Стадия Discovery происходит в 4 этапа:

1. Initiation**.** Клиент передаёт инициирующее сообщение (Active Discovery Initiation, PADI) по широковещательному адресу канального уровня (FF:FF:FF:FF:FF:FF).
2. Offer. Один или несколько серверов передают сообщение-предложение (Active Discovery Offer, PADO) на аренду MAC-адрес клиента.
3. Request. Клиент передаёт сообщение о запросе сеанса (Active Discovery Request, PADR) по MAC-адресу выбранного сервера.
4. Confirmation. Выбранный сервер передаёт сообщение о подтверждении (Active Discovery Session-confirmation , PADS) установлении сеанса.

На этом этапе заканчивается первая стадия.

Существует 5 видов PPPoE-сообщений:

1. Active Discovery Initiation (PADI) – начало поиска клиентом сервера.
2. Active Discovery Offer (PADO) – оповещение клиента о наличии сервера.

3. Active Discovery Request (PADR) – запрос клиента на установление соединения.

4. Active Discovery Session-confirmation (PADS) – подтверждение установления сеанса связи сервером.

5. Active Discovery Terminate (PADT) – завершение соединения.

Вторая стадия представляет из себя PPP-сеанс связи. Отличие PPPoE от PPP заключается в том, что блоки данных передаются не по последовательной линии, а по сети Ethernet. Заголовок PPPoE занимает 8 байт, что необходимо учитывать при расчёте MTU (1500-8=1492).

Практическая часть

Цель работы:
Изучение протокола PPPoE и способов его настройки и использования в ОС Linux и брандмауэре ASA5505.

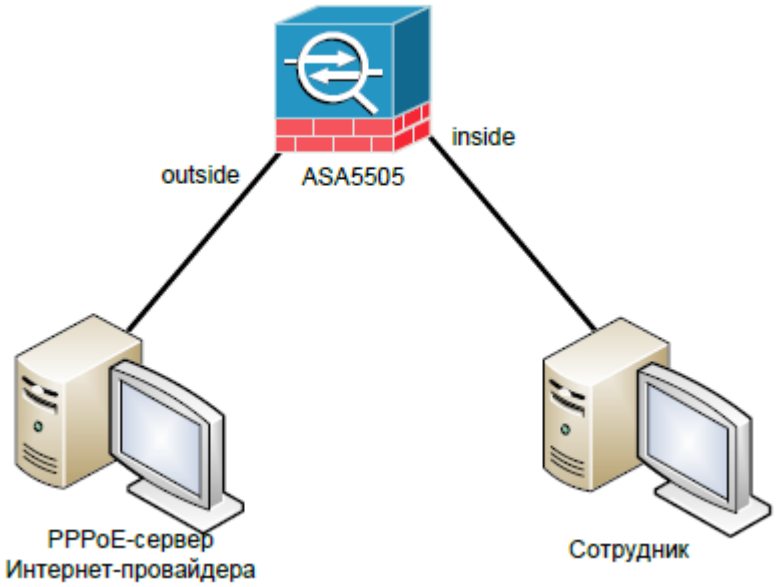


Рисунок.

Порядок выполнения работы:
1. Соберите топологию сети, представленную на рисунке.

2. Настройте рабочие станции и брандмауэр таким образом, чтобы интерфейс outside ASA5505 и PPPoE-сервер принадлежали одной IP-подсети, а интерфейс inside ASA5505 и машина сотрудника – другой.

3. Используя утилиту **rp-pppoe**, настройте PPPoE-сервер на машине Интернет-провайдера.

4. Настройте ASA5505 в качестве PPPoE-клиента (используя созданную учетную запись пользователя). Установите PPPoE-туннель.

5. Осуществите доступ с машины сотрудника в сеть Интернет, то есть к машине провайдера.

Литература

1. James Boney, Cisco IOS in a Nutshell, 2-nd Ed., O`Reilly, 2008
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2008
3. НПП «Учтех-Профи», ОС Arch Linux, Лабораторный практикум, Челябинск, 2010