System i

Службы удаленного доступа: Соединения PPP

версия 6 выпуск 1

System i

Службы удаленного доступа: Соединения PPP

версия 6 выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 69.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761–SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

© Copyright International Business Machines Corporation 1998, 2008. Все права защищены.

Содержание

© Copyright IBM Corp. 1998, 2008

Службы удаленного доступа: Соединения PPP

Двухточечный протокол (PPP) - это стандарт Internet для передачи данных по последовательным линиям.

PPP - это наиболее распространенный протокол, который поддерживается большинством провайдеров Internet (ISP). PPP позволяет компьютерам подсоединяться к сетям. Сети в свою очередь обеспечивают доступ к Internet. System i поддерживает TCP/IP PPP в качестве компонента связи в глобальных сетях (WAN).

Протокол PPP позволяет удаленным системам обмениваться данными с платформой System i. С помощью PPP удаленные системы, подключенные к системе, могут получить доступ к ресурсам сервера или другим системам в той же сети, что и сервер. Кроме того, саму систему можно настроить для подключения к Internet по протоколу PPP. Мастер настройки коммутируемых соединений System i Navigator поможет вам последовательно выполнить операции по подключению системы к сети Internet или к внутренней сети.

Документ в формате PDF для Служб удаленного доступа.

Файл PDF этой информации можно просмотреть и напечатать.

Для просмотра или загрузки этого документа в формате PDF щелкните на ссылке Службы удаленного доступа: соединения PPP (940 Кб).

Сохранение файлов PDF

Для сохранения файла PDF на рабочей станции (для последующего просмотра и печати) выполните следующие действия:

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Щелкните на **Сохранить**.

Загрузка программы Adobe Reader

Для просмотра и печати этих PDF-файлов требуется программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe по адресу (www.adobe.com/products/acrobat/readstep.html)

.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Принципы работы PPP

Двухточечный протокол (PPP) применяется для соединения платформы System i с удаленными сетями, клиентскими PC, другими платформами System i или провайдером Internet (ISP). Для успешной работы с протоколом необходимо знать как возможности самого протокола, так и особенности его поддержки в i5/OS.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

© Copyright IBM Corp. 1998, 2008

Что такое PPP?

Двухточечный протокол (PPP) - это протокол TCP/IP, применяемый для соединения двух компьютерных систем. Системы в сети Internet могут устанавливать друг с другом соединение по телефонным линиям с помощью двухточечного протокола, или PPP.

Протокол PPP подразумевает физическое соединение двух систем по телефонной линии. Например, соединение PPP между сервером в филиале компании и сервером в центральном офисе позволяет передавать данные из одной системы в другую.

PPP позволяет взаимодействовать сетевому программному обеспечению от различных производителей. Кроме того, с его помощью несколько сетевых протоколов могут использовать одну линию связи.

Протокол PPP подробно описан в следующих документах RFC. Дополнительная информация приведена по адресу RFC Editor.

- RFC-1661 Протокол двухточечной связи (PPP)
- RFC-1662 PPP on HDLC-like framing
- RFC-1994 PPP CHAP

Профайлы соединений

Профайлы двухточечных (PPP) соединений задают набор параметров и ресурсов для конкретного соединения PPP. Эти профайлы можно применять для входящих или для исходящих соединений PPP.

Можно использовать два типа профайлов, позволяющих определить набор характеристик соединения PPP или набора соединений:

- *Профайлы исходящих соединений* - это профайлы двухточечных соединений, которые устанавливаются локальной системой с удаленной системой. С помощью этого объекта можно настраивать исходящие соединения.
- *Профайлы входящих соединений* - это профайлы двухточечных соединений, которые устанавливаются удаленной системой с локальной системой. С помощью этого объекта можно настраивать входящие соединения.

Профайл соединения определяет работу соединения PPP. Профайл соединения содержит ответы на следующие вопросы:

- Какой протокол соединения вы используете? (PPP или SLIP)
- Должна ли система устанавливать соединение с удаленным компьютером (быть инициатором)? Должна ли система ожидать вызова удаленной системы (быть отвечающей стороной)?
- Какая линия связи применяется этим соединением?
- Каким образом система должна определять IP-адрес?
- Каким образом система должна идентифицировать удаленную систему? Где должна храниться идентификационная информация системы?

Профайл соединения содержит информацию о следующих параметрах соединения:

- Тип профайла и линии связи
- Параметры многоканального соединения
- Номера удаленных телефонов и опции набора номера
- Сведения об идентификации
- Параметры TCP/IP: IP-адреса, маршрутизация и фильтрация IP-пакетов
- Управление работой и настройка соединений
- Сервер имен доменов

Система хранит эту параметры конфигурации в профайле соединения. Эта информация позволяет системе устанавливать соединение PPP с другими системами. В профайле соединения содержится следующая информация:

- **Тип протокола**.Можно выбрать протокол PPP или SLIP. IBM рекомендует применять протокол PPP.
- **Режим**.Тип соединения и режим работы для данного профайла соединения.

  Тип соединения. Задает тип линии, применяемой соединением, а также способ установления связи (набор номера или ответ) для исходящих и входящих соединений, соответственно. Вы можете указать следующий тип соединения:

  – Коммутируемая линия
  – Выделенная линия
  – Протокол туннеля второго уровня (L2TP) (виртуальная линия)
  – Двухточечный протокол по Ethernet (PPPoE) (виртуальная линия)

  Службы PPPoE применимы только для профайлов входящих соединений.
- **Режим работы**. Возможные режимы работы зависят от типа соединения.

Таблица 1. Возможные режимы работы для входящих соединений

Тип соединения	**Возможные режимы работы**
Коммутируемая линия	• Набор номера • Набор номера по запросу (только набор номера) • Набор номера по запросу (отдельный узел с возможностью ответа) • Набор номера по запросу (с поддержкой нескольких удаленных систем)
Выделенная линия	Вызов
L2TP	• Вызов • Транзитный вызов • Удаленный набор номера
Двухточечное соединение (PPP) по Ethernet	Вызов

Таблица 2. Возможные режимы работы для исходящих соединений

Тип соединения	**Возможные режимы работы**
Коммутируемая линия	Ответ
Выделенная линия	Ответ
L2TP	Ответ (Сетевой сервер)

- **Конфигурация линии связи**.Этот параметр задает тип физической линии, применяемой данным соединением.

  Он зависит от выбранного режима соединения. Для коммутируемой и выделенной линии можно выбрать следующие типы линий связи:

  – Отдельная линия
  – Пул линий

  Для всех прочих типов соединений (выделенная линия, L2TP, PPPoE) единственным вариантом является Отдельная линия.

Ссылки, связанные с данной

“Требования к программному и аппаратному обеспечению” на стр. 32
Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров - платформа System i, может быть как инициатором, так и обработчиком соединения.

Поддержка групповых стратегий

Используя поддержку групповых стратегий, администратор сети может определять пользовательские групповые стратегии для управления ресурсами. Индивидуальным пользователям можно назначать стратегии контроля доступа при входе по протоколу PPP или L2TP.

Все пользователи могут быть разделены на категории, каждой из которых создается отдельная стратегия, позволяющая задавать свои ограничения на используемые ресурсы, например, число линий в комплекте из нескольких линий, атрибуты (такие как пересылка IP-пакетов) и набор правил фильтрации IP-пакетов. Поддержка групповых стратегий позволяет администраторам также определить, например, группу обычных пользователей, доступ которых к ресурсам Internet не ограничен, и группу корпоративных пользователей, которым предоставляется доступ лишь к некоторым сайтам и службам.

Ссылки, связанные с данной

“Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

“Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23
Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Сценарии: Удаленный доступ с помощью соединения PPP

Данные сценарии описывают работу протокола PPP и применение среды PPP в сети. В описанных в этих сценариях основных принципах PPP содержится информация, которая будет полезна как начинающим, так и опытным пользователям. С этой информацией рекомендуется ознакомиться до начала планирования и настройки соединений PPP.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Пример: Применение PPP и DHCP на одном System i

Приведена информация по настройке моделиSystem i как сервера DHCP в локальной сети и для удаленных клиентов.

Удаленным клиентам, таким как подключающиеся по модему, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к модели System i с помощью соединения по Протоколу двухточечной связи (PPP). Для того чтобы получить доступ в сеть, клиент, подключающийся по модему, должен получить информацию IP, как и клиент, напрямую подключенный к сети. Сервер DHCP System i может предоставлять информацию об IP-адресе клиенту PPP, подключающемуся по модему, как и любому клиенту, подключенному напрямую. На рисунке показан удаленный клиент, которому требуется подключиться по модему к сети компании и выполнить какую-то работу.

Рисунок 1. Применение PPP и DHCP на одной модели System i

Для того чтобы удаленный сотрудник успешно стал частью сети компании, модельSystem i должен использовать сочетание служб удаленного доступа и DHCP. Службы удаленного доступа обеспечивают подключение по модему к моделиSystem i. Если все настроено верно, то после того как клиент установит соединение, сервер PPP прикажет серверу DHCP передать информацию TCP/IP клиенту.

В этом примере одна стратегия подсети DHCP относится к локальным и к удаленным клиентам.

Если требуется, чтобы профайл PPP обращался к DHCP за присвоением IP, сделайте это в профайле PPP. В параметрах TCP/IP профайла входящего соединения задайте метод присвоения IP-адресов вместо Фиксированного равным DHCP. Для того чтобы удаленные клиенты могли обращаться к другим клиентам сети, таким как принтер LAN, необходимо также разрешить пересылку IP в параметрах TCP/IP профайла и в свойствах стека TCP/IP. Если пересылка IP включена только в профайле PPP, то модель System i не будет передавать IP-пакеты. Необходимо задать пересылку IP и а профайле, и в стеке.

Кроме того, IP-адрес локального интерфейса в профайле PPP должен быть IP-адресом, входящим в определение подсети на сервере DHCP. В этом примере адрес локального интерфейса профайла PPP должен быть равен 10.1.1.1. Этот адрес нужно также исключить из пула адресов сервера DHCP, чтобы он не был присвоен никакому клиенту DHCP.

Планирование настройки DHCP для локальных клиентов и клиентов PPP

Таблица 3. Глобальные параметры конфигурации (для всех клиентов сервера DHCP)

Объект		**Значение**
Параметры конфигурации	Параметр 1: маска подсети	255.255.255.0
	Параметр 6: сервер DNS	10.1.1.1
	Параметр 15: имя домена	mycompany.com
Выполняет ли система обновления DNS?		Нет
Поддерживает ли система клиента BOOTP?		Нет

Таблица 4. Подсеть для локальных клиентов и клиентов PPP

Объект		**Значение**
Имя подсети		MainNetwork
Адреса для управления		10.1.1.3 - 10.1.1.150
Время действия адреса		24 часа (по умолчанию)
Параметры конфигурации	Унаследованные параметры	Параметры глобальной конфигурации
Адреса подсети, не присваиваемые сервером		10.1.1.1 (Адрес локального интерфейса, указанный в параметрах TCP/IP свойств профайла входящего соединения в System i Navigator)

Прочие параметры

- Метод задания удаленного IP-адреса для DHCP в профайле входящего соединения PPP.
  1. Разрешите подключение клиенту DHCP WAN к серверу DHCP или пересылку соединения, используя пункт меню **Службы** для Служб удаленного доступа в System i Navigator.
  2. Выберите Использовать DHCP для назначения IP-адресов в Свойствах TCP/IP профайла входящего соединения в System i Navigator.
- Разрешите удаленным системам доступ к другим сетям (IP forwarding) в Свойствах TCP/IP профайла входящего соединения в System i Navigator.
- Разрешите пересылку дейтаграмм IP в Свойствах TCP/IP в System i Navigator.

Пример: Профайлы DHCP и PPP на разных моделях System i.

Приведена информация о том, как настроить две модели System i как сервер DHCP и промежуточный агент DHCP/BOOTP для двух локальных сетей и удаленных клиентов, подключающихся по телефонной линии.

Пример, описывающий PPP и DHCP в одной модели System i, проиллюстрировал, каким образом PPP и DHCP в одной системе разрешают удаленных доступ клиентов к сети. По соображениям физической структуры сети или защиты сети часто бывает желательно разнести серверы PPP и DHCP или иметь выделенный сервер PPP без служб DHCP. На рисунке ниже показана сеть, к которой подключаются клиенты по телефонной линии, но службы PPP и DHCP разнесены на разные серверы.

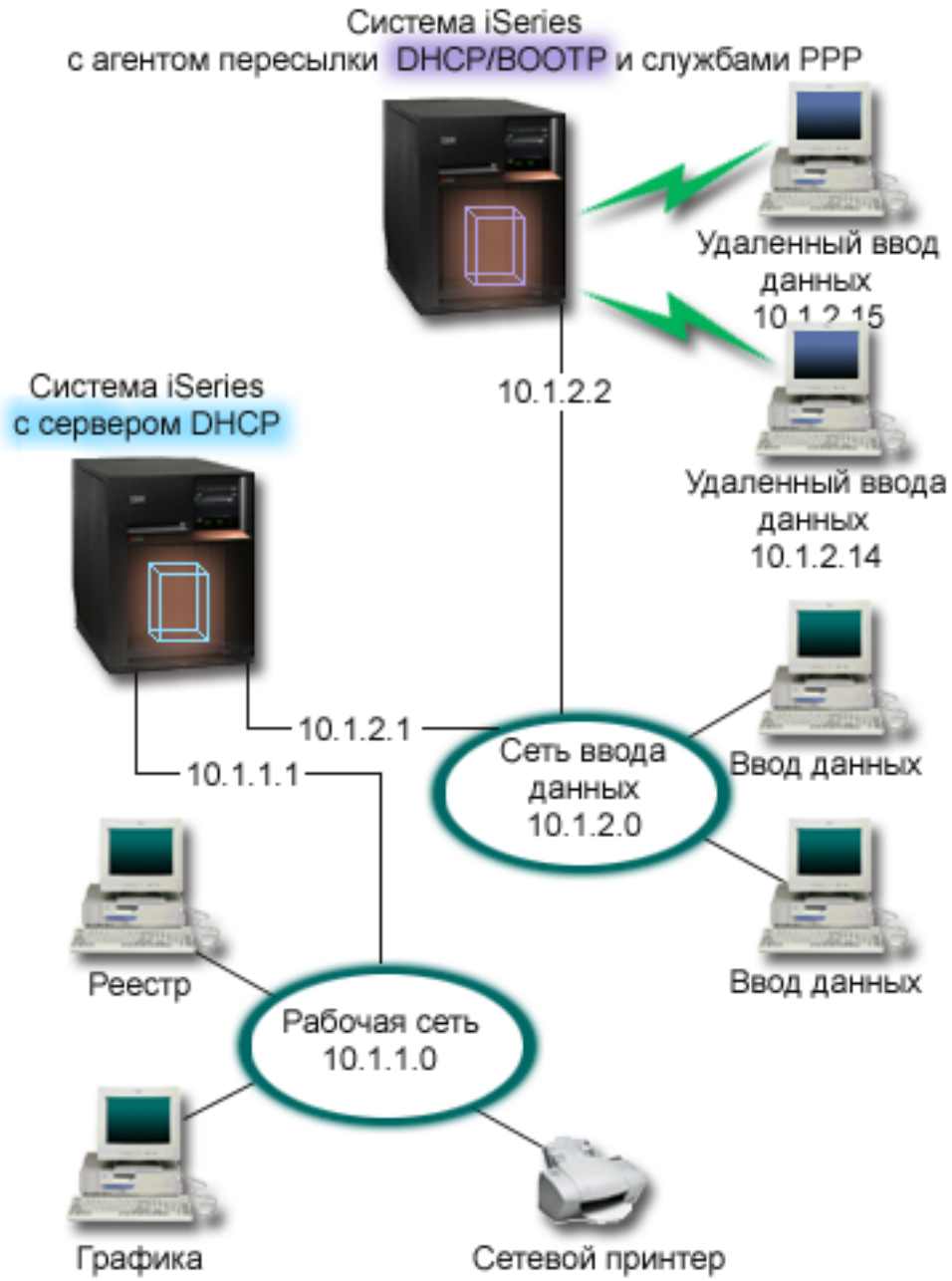


Рисунок 2. Профайлы DHCP и PPP на разных моделях System i.

Клиенты записей удаленных данных дозваниваются по модему на сервер PPP System i. Профайл PPP на этом сервере должен иметь метод удаленного IP-адреса, как DHCP в примере PPP и DHCP на одной модели System i. Профайл PPP и свойства стека TCP/IP на сервере PPP должны иметь пересылку IP. Поскольку этот сервер работает еще и как промежуточный агент DHCP, должен быть включен сервер TCP/IP промежуточного агента. Это позволяет серверу удаленного доступа System i передавать пакеты DHCPDISCOVERDISCOVER серверу DHCP. Сервер DHCP ответит и распределит информацию TCP/IP клиентам, подключающимся по модему к серверу PPP.

Сервер DHCP присваивает IP-адреса для сетей 10.1.1.0 и 10.1.2.0. В сети записи данных сервер DHCP присваивает IP-адреса от 10.1.2.10 до 10.1.2.40 клиентам, подключающимся по модему или прямо

подключенным к сети. Клиентам записи данных также требуется адрес маршрутизатора (параметр 3) 10.1.2.1, чтобы связываться с рабочей сетью, и на сервере DHCP System i должна быть включена пересылка IP.

Кроме того, IP-адрес локального интерфейса в профайле PPP должен быть IP-адресом, входящим в определение подсети на сервере DHCP. В этом примере адрес локального интерфейса профайла PPP должен быть равен 10.1.2.2. Этот адрес нужно также исключить из пула адресов сервера DHCP, чтобы он не был присвоен никакому клиенту DHCP.IP-адрес локального интерфейса должен быть адресом, на который сервер DHCP может отправлять пакеты ответов.

Планирование настройки DHCP для DHCP с промежуточным агентом DHCP

Таблица 5. Глобальные параметры конфигурации (для всех клиентов сервера DHCP)

Объект		**Значение**
Параметры конфигурации	Параметр 1: маска подсети	255.255.255.0
	Параметр 6: сервер DNS	10.1.1.1
	Параметр 15: имя домена	mycompany.com
Выполняет ли система обновления DNS?		Нет
Поддерживает ли система клиента BOOTP?		Нет

Таблица 6. Подсеть для рабочей сети

Объект		**Значение**
Имя подсети		WorkNetwork
Адреса для управления		10.1.1.3 - 10.1.1.150
Время действия адреса		24 часа (по умолчанию)
Параметры конфигурации	Унаследованные параметры	Параметры глобальной конфигурации
Адреса подсети, не присваиваемые сервером		нет

Таблица 7. Подсеть для Сети входных данных

Объект		**Значение**
Имя подсети		DataEntry
Адреса для управления		10.1.2.10 - 10.1.2.40
Время действия адреса		24 часа (по умолчанию)
Параметры конфигурации	Параметр 3: маршрутизатор	10.1.2.1
	Унаследованные параметры	Параметры глобальной конфигурации
Адреса подсети, не присваиваемые сервером		10.1.2.1 (маршрутизатор) 10.1.2.15 (IP-адрес локального интерфейса клиента удаленной сети входных данных) 10.1.2.14 (IP-адрес локального интерфейса клиента удаленной сети входных данных)

Дополнительная настройка на платформе System i, на которой работает PPP

- Настройка пересылочного сервера BOOTP/DHCP

Объект	**Значение**
Адрес интерфейса	10.1.2.2
IP-адрес сервера - получателя пакетов	10.1.2.1

- Метод задания удаленного IP-адреса для DHCP в профайле входящего соединения PPP
  1. Разрешите подключение клиенту DHCP WAN к серверу DHCP или пересылку соединения, используя пункт меню Службы для Служб удаленного доступа в System i Navigator.
  2. Выберите Использовать DHCP для назначения IP-адресов в Свойствах TCP/IP профайла входящего соединения в System i Navigator
- Разрешите удаленным системам доступ к другим сетям (IP forwarding) в Свойствах TCP/IP профайла входящего соединения в System i Navigator. Это позволяет удаленным клиентам иметь доступ к сети входных данных.
- Разрешите пересылку дейтаграмм IP в Свойствах TCP/IP в System i Navigator. Это позволяет удаленным клиентам иметь доступ к сети входных данных.

Защита туннеля L2TP с помощью IPSec

В этом сценарии рассматривается соединение между хостом, расположенным в филиале фирмы, и корпоративным сервером. Соединение устанавливается по туннелю L2TP, защищенному с помощью IPSec. Хосту филиала IP-адрес назначается динамически, тогда как у корпоративного сервера есть постоянный внешний IP-адрес.

Описание задачи

Предположим, что у вашей фирмы открыт небольшой филиал в другом регионе страны. В любой момент в течение рабочего дня филиалу может потребоваться конфиденциальная информация, хранящаяся на модели System i, которая подключена к корпоративной сети. Для подключения филиала к корпоративной сети применяется дорогая выделенная линия связи. Хотя защищенное соединение с корпоративной сетью фирмы необходимо для работы филиала, было бы желательно сократить стоимость такого соединения. Это можно сделать с помощью необязательного туннеля L2TP, за счет которого можно расширить корпоративную сеть таким образом, чтобы в нее входил филиал фирмы. Для защиты данных, передаваемых по туннелю L2TP, применяется функция VPN.

Применение необязательного туннеля L2TP дает возможность удаленному филиалу напрямую устанавливать защищенное соединение с сетевым сервером L2TP (LNS), расположенным в корпоративной сети. При этом на клиенте будет расположен концентратор L2TP (LAC). Туннель будет прозрачен для провайдера Internet (ISP) удаленного клиента, поэтому не требуется, чтобы ISP поддерживал протокол L2TP. Для получения дополнительной информации о протоколе L2TP обратитесь к разделу Протокол L2TP.

Важное замечание: В данном сценарии рассматриваются шлюзы, которые напрямую подключены к Internet. Для простоты предполагается, что брандмауэр отсутствует. Это не означает, что брандмауэр использовать не нужно. Вы должны оценить все опасности, связанные с подключением к Internet.

Цели

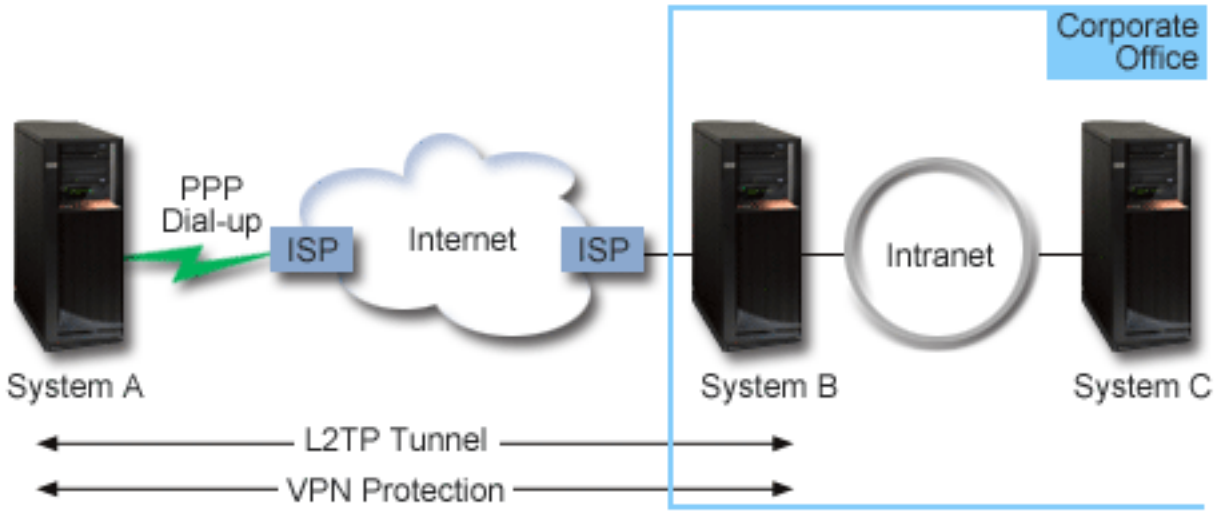
В данном сценарии система, расположенная в филиале фирмы, подключается к корпоративной сети с помощью защищенного туннеля L2TP, который устанавливается через шлюз.

В этом сценарии преследуются следующие цели:

- Соединение с корпоративной сетью всегда устанавливается системой, расположенной в филиале фирмы.
- В сети филиала фирмы есть только одна система, которой требуется доступ к корпоративной сети. Такая система играет в сети филиала роль хоста, а не шлюза.
- Корпоративный сервер - это хост, подключенный к корпоративной сети.

Подробности

На приведенном ниже рисунке показана сеть, описанная в этом сценарии:



Система A

- Есть права доступа к приложениям TCP/IP всех систем, подключенных к корпоративной сети.
- IP-адрес назначается динамически провайдером Internet.
- Поддерживает протокол L2TP.

Система B

- Есть права доступа к приложениям TCP/IP в системе A.
- Адрес подсети равен 10.6.0.0, маска подсети равна 255.255.0.0. Эта подсеть является конечной точкой данных туннеля VPN в корпоративной сети.
- Для подключения к Internet применяется IP-адрес 205.13.237.6. Этот адрес представляет конечную точку соединения. Это означает, что система B отвечает за управление ключами и применение правил IPSec к принимаемым и отправляемым дейтаграммам IP. Система B соединяется со своей подсетью с IP-адресом 10.6.11.1.

Если говорить в терминах L2TP, то *Система A* играет роль инициатора L2TP, а *Система B* играет роль конечной системы L2TP.

Задачи настройки

Предполагается, что в системах уже заданы правильные параметры TCP/IP. Необходимо выполнить следующие задачи:

Сценарий: Подключение системы к концентратору PPPoE

Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

Ситуация

Вам требуется более быстродействующее соединение с Internet, и вы рассматриваете вариант подключения к локальному ISP (провайдеру Internet) по линии DSL. В настоящее время локальный ISP подключает клиентов

с помощью PPPoE. Вы хотели бы использовать это соединение PPPoE для установки высокоскоростного соединения с Internet через систему.

Рисунок 3. Подключение системы к ISP с помощью PPPoE

Способ устранения

Система может установить соединение PPPoE с локальным ISP. Система использует новый тип виртуальной линии PPPoE, связанной с физической линией Ethernet с адаптером Ethernet типа 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A или 576A. Этот тип виртуальных линий поддерживает сеансы PPP по локальной сети Ethernet, подключенной к модему DSL, который является шлюзом к удаленному ISP. Этот шлюз позволяет пользователям, подключенные к локальной сети, иметь высокоскоростной доступ к Internet с помощью соединения PPPoE. После установления соединения между системой и провайдером Internet (ISP) пользователи LAN получают доступ к ISP по соединению PPPoE, используя IP-адрес системы. С целью обеспечения дополнительной защиты для виртуальной линии PPPoE можно определить правила фильтрации, ограничивающие входящий поток данных из Internet.

Пример конфигурации

Для настройки примера конфигурации PPP в System i Navigator выполните следующие действия:

1. Настройте устройство, через которое устанавливается соединение с ISP.
2. Настройте профайл исходящего соединения в системе.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: PPP через Ethernet
   - **Режим работы**: Вызов
   - **Конфигурация канала связи**: Одна линия
3. На странице Общие страницы свойств нового профайла PPP введите имя и описание профайла исходящего соединения PPP. Это имя будет относиться и к профайлу соединения, и к виртуальной линии PPPoE.

4. Нажмите кнопку **Соединение**, чтобы открыть страницу Соединение. Выберите **имя виртуальной линии PPPoE**, соответствующее имени этого профайла соединения. После выбора линии в System i Navigator появится окно **свойства линии**.
   a. На странице Общие введите описание виртуальной линии PPPoE.
   b. Нажмите кнопку **Ссылка**, чтобы открыть страницу Ссылка. В списке имен физических линий выберите линию Ethernet для данного соединения и нажмите **Открыть**. Если вы хотите определить новую линию Ethernet, введите ее имя и нажмите **Создать**. System i Navigator будет показано окно **Свойства линии Ethernet**.

      Примечание: Для PPPoE требуется адаптер Ethernet типа 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A или 576A.

      1) На странице Общие введите описание линии Ethernet и убедитесь в том, что линия использует предполагаемые аппаратные ресурсы.
      2) Нажмите кнопку **Ссылка**, чтобы открыть страницу Ссылка. Введите свойства физической линии Ethernet. Дополнительная информация приведена в соответствующем разделе электронной справки и в документации по адаптеру Ethernet.
      3) Нажмите кнопку **Прочее**, чтобы открыть страницу Прочее. Укажите уровень доступа и права доступа, предоставляемые другим пользователям.
      4) Нажмите **OK** для возврата на страницу Свойства виртуальной линии PPPoE.
   c. Нажмите кнопку **Ограничения**, чтобы задать параметры идентификации LCP, или кнопку **OK**, чтобы вернуться на страницу Создать соединение PPP.
   d. После возврата на страницу Соединение настройте адресацию сервера PPPoE на основе данных, предоставленных провайдером (ISP).
5. Если вы хотите, чтобы система идентифицировала себя при подключении к ISP или чтобы система идентифицировала удаленный сервер, перейдите на страницу **Идентификация**.
6. Нажмите кнопку **Параметры TCP/IP**, чтобы открыть страницу TCP/IP, и выберите параметры обработки IP-адресов для этого профайла соединения. Значения параметров должны быть предоставлены провайдером Internet (ISP). Для того чтобы пользователи LAN могли подключаться к ISP с помощью IP-адресов, выделенных системе, выберите пункт **Скрыть адреса (Полная маскировка)**.
7. Откройте страницу **DNS** и введите IP-адрес сервера DNS, предоставленный провайдером.
8. Для создания профайла нажмите **OK**.

Понятия, связанные с данным

“Поддержка групповых стратегий” на стр. 4
Используя поддержку групповых стратегий, администратор сети может определять пользовательские групповые стратегии для управления ресурсами. Индивидуальным пользователям можно назначать стратегии контроля доступа при входе по протоколу PPP или L2TP.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Ссылки, связанные с данной

“Конфигурация линии связи” на стр. 52
Конфигурация линии связи задает тип линии, применяемый для создания соединения PPP.

“Идентификация систем” на стр. 45
Соединения PPP с платформой System i предусматривают несколько вариантов идентификации как удаленных клиентов, подключающихся к системе, так и соединений с провайдером Internet (ISP) или с другим сервером, к которому система.

“Обработка IP-адресов” на стр. 42
Соединения PPP предоставляют несколько вариантов обработки IP-адресов в зависимости от типа профайла соединения.

“Фильтрация IP-пакетов” на стр. 42
Фильтрация IP-пакетов позволяет ограничить доступ отдельного пользователя к различным службам при работе этого пользователя в сети.

Сценарий: Подключение удаленных клиентов к системе

Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

Ситуация

Как администратор сети компании, вы должны поддерживать в рабочем состоянии свою систему и клиентов сети. В этом случае вам наверняка понравится возможность устранять неполадки, не приходя в офис компании, например, из дома. Допустим, что офис компании не подключен к сети Internet-bound, и подключаться к системе можно с помощью соединений PPP. Кроме того, единственным модемом в системе является модем 7852-400 ECS, и его можно применить для создания соединения.

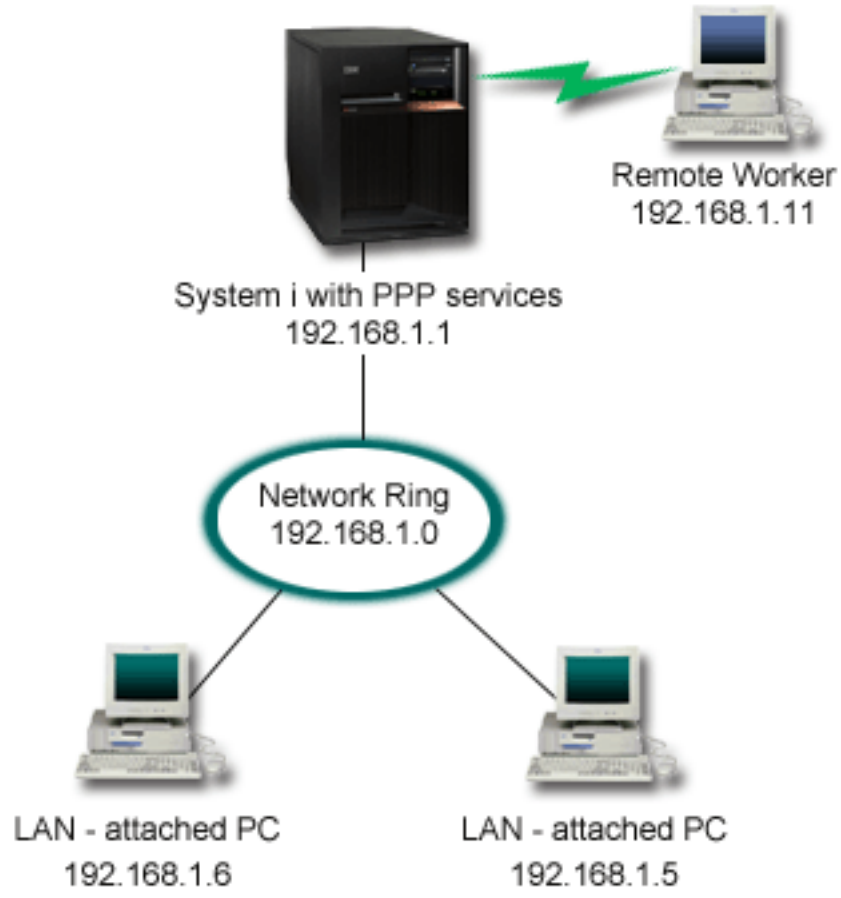


Рисунок 4. Подключение удаленных клиентов к системе

Способ устранения

Домашний PC можно подключить к системе с помощью соединения PPP и модема. Поскольку для создания соединений PPP этого типа применяется модем электронной поддержки заказчиков (ECS), то необходимо убедиться, что модем настроен для работы как в синхронном, так и в асинхронном режимах. На рисунке

показана система с двумя службами PPP, подключенный к локальной сети с двумя PC. Удаленный обработчик затем соединяется с локальной системой. Локальная система идентифицируется и становиться частью рабочей сети (192.168.1.0). В этом случае проще всего будет присвоить удаленному клиенту статический IP-адрес.

Удаленный обработчик использует Протокол идентификации с квитированием связи по вызову (CHAP-MD5) для идентификации в системе. Применение MS_CHAP в системе невозможно, поэтому необходимо убедиться в том, что клиент PPP применяет CHAP-MD5.

Для подключения удаленных пользователей к сети компании по описанной выше схеме необходимо включить пересылку IP-пакетов как в стеке TCP/IP, так и в профайле входящих соединений PPP, и настроить IP-маршрутизацию. Для ограничения или защиты действий удаленного пользователя в сети можно применять правила фильтрации IP-пакетов.

На рисунке показан только один удаленный клиент, так как модем Электронной поддержки заказчиков (ECS) не поддерживает несколько параллельных соединений.

Пример конфигурации

Для настройки примера конфигурации PPP в System i Navigator выполните следующие действия:

1. Настройте удаленный доступ к сети и создайте модемное соединение с удаленным PC.
2. Настройте профайл входящего соединения в системе.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: Коммутируемая линия
   - **Режим работы**: Ответ
   - **Конфигурация линии связи**: В зависимости от применяемой среды, это может быть отдельная линия или пул линий.
3. На странице Общие страницы свойств нового профайла PPP введите имя и описание профайла входящего соединения PPP.
4. Нажмите кнопку **Соединение**, чтобы открыть страницу Соединение. Выберите **Имя линии** или создайте новую линию с помощью кнопки **Создать**.
   a. На странице Общие выберите существующий аппаратный ресурс, к которому подключен адаптер 7852–400, и укажите в поле Обработка кадров значение **Асинхронная**.
   b. Нажмите кнопку **Модем**, чтобы открыть страницу Модем. В списке имен модемов выберите модем **IBM 7852–400**.
   c. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
5. Нажмите кнопку **Идентификация**, чтобы открыть страницу Идентификация.
   a. Выберите **Обязательная проверка и идентификация удаленных систем сервером iSeries**.
   b. Выберите **Идентификация с помощью контрольного списка** и добавьте нового удаленного пользователя в контрольный список.
   c. Выберите опцию **Разрешить шифрование паролей (CHAP-MD5)**.
6. Нажмите кнопку **Параметры TCP/IP**, чтобы открыть страницу TCP/IP.
   a. Задайте локальный IP-адрес 192.168.1.1.
   b. Для удаленных IP адресов выберите **Фиксированный IP-адрес** с начальным IP адресом 192.168.1.11.
   c. Выберите опцию **Предоставить удаленной системе доступ к другим сетям**.
7. Для создания профайла нажмите **OK**.

Понятия, связанные с данным

“Планирование PPP” на стр. 32
Планирование протокола двухточечной связи (PPP) подразумевает создание соединений PPP и администрирование ими.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Ссылки, связанные с данной

“Протокол идентификации с квитированием связи по вызову с MD5” на стр. 45
Протокол CHAP-MD5 с помощью алгоритма MD-5 вычисляет псевдослучайное значение, которое известно только проверяющей системе и удаленному устройству.

“Конфигурация линии связи” на стр. 52
Конфигурация линии связи задает тип линии, применяемый для создания соединения PPP.

“Пул линий” на стр. 53
Выберите этот тип для создания соединения PPP с применением линии из пула линий. При создании соединения PPP система выбирает из пула незанятую линию. Для профайлов набора номера по запросу линия не выбирается до тех пор, пока система не обнаружит пакеты TCP/IP, которые необходимо отправить удаленной системе.

Сценарий: Подключение локальной сети к Internet с помощью модема

Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Систему можно подключить к ISP с помощью модема. Клиенты PC, подключенные к сети, будут использовать операционную систему i5/OS в качестве шлюза при доступе к Internet.

Ситуация

Пользователям вашей корпоративной сети необходим доступ к Internet. Если при этом не планируется интенсивный обмен данными, то систему и клиентов PC LAN можно подключить к Internet с помощью модема. На следующем рисунке приведен пример такой ситуации.

Рисунок 5. Подключение локальной сети к Internet с помощью модема

Способ устранения

Для подключения системы к провайдеру Internet (ISP) можно использовать интегрированный модем или любой другой совместимый модем. Для подключения системы к ISP с помощью соединения PPP необходимо создать профайл инициатора соединения PPP.

При подключении системы к ISP клиенты PC в локальной сети могут работать в Internet, используя систему в качестве шлюза. В профайле исходящего соединения необходимо включить опцию Скрыть адреса, чтобы клиенты локальной сети с частными IP-адресами могли установить соединение с Internet.

При подключении системы локальной сети к Internet необходимо обратить внимание на возможные связанные с этим опасности. Обратитесь к провайдеру Internet и согласуйте с ним действия и стратегии защиты.

В зависимости от объема данных, получаемых и отправляемых в Internet, полоса пропускания соединения может стать недостаточной.

Пример конфигурации

Для настройки примера конфигурации в System i Navigator выполните следующие действия:

1. Настройте профайл исходящего соединения в системе.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: Коммутируемая линия
   - **Режим работы**: Набор номера
   - **Конфигурация линии связи**: В зависимости от применяемой среды, это может быть отдельная линия или пул линий.
2. На странице Общие страницы свойств нового профайла PPP введите имя и описание профайла исходящего соединения PPP.
3. Нажмите кнопку **Соединение**, чтобы открыть страницу Соединение. Выберите соответствующее имя линии или введите новое имя с помощью кнопки **Создать**.
   a. На странице Общие свойств новой линии выберите существующий аппаратный ресурс. При выборе ресурса внутреннего модема тип и способ обработки кадров будут заданы автоматически.
   b. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
4. Для установления соединения с ISP нажмите кнопку **Добавить** и введите номер телефона провайдера. Убедитесь в том, что номер введен с правильным префиксом.
5. Нажмите кнопку **Идентификация**, чтобы открыть станицу Идентификация, и выберите опцию **Разрешить удаленной системе идентификацию сервера iSeries**. Выберите протокол идентификации и введите имя пользователя и пароль.
6. Нажмите кнопку **Параметры TCP/IP**, чтобы открыть страницу TCP/IP.
   a. Выберите опцию **Назначается удаленной системой** как для удаленного, так и для локального IP-адресов.
   b. Выберите опцию **Добавить удаленную систему в маршрут по умолчанию**.
   c. Отметьте переключатель **Скрыть адреса**, чтобы пакеты для локальных IP-адресов не пересылались в Internet.
7. Откройте страницу **DNS** и введите IP-адрес сервера DNS, предоставленный провайдером.
8. Для создания профайла нажмите **OK**.

Для подключения к Internet с помощью этого профайла щелкните на нем правой кнопкой мыши в System i Navigator и выберите **Запустить**. После установления соединения состояние профайла изменится на **Активно**.Обновите информацию на экране.

Примечание: Кроме того, необходимо убедиться, что для остальных систем в сети правильно задана маршрутизация, и пакеты TCP/IP, предназначенные для Internet, отправляются через систему.

Понятия, связанные с данным

“Планирование PPP” на стр. 32
Планирование протокола двухточечной связи (PPP) подразумевает создание соединений PPP и администрирование ими.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Ссылки, связанные с данной

“Пул линий” на стр. 53
Выберите этот тип для создания соединения PPP с применением линии из пула линий. При создании

соединения PPP система выбирает из пула незанятую линию. Для профайлов набора номера по запросу линия не выбирается до тех пор, пока система не обнаружит пакеты TCP/IP, которые необходимо отправить удаленной системе.

“Конфигурация линии связи” на стр. 52
Конфигурация линии связи задает тип линии, применяемый для создания соединения PPP.

Сценарий: Подключение сети филиала компании к основной сети с помощью модема

Модем позволяет обмениваться данными между двумя расположениями (такими, например, как центральный офис и филиал). Две сети можно объединить с помощью соединения PPP, подключив одну сеть к системе в центральном офисе, а другую - к другой в офисе филиала компании.

Ситуация

Основной офис и филиал компании находятся в разных зданиях. Серверу в филиале компании необходимо каждый день подключаться к серверу в главном офисе для обмена информацией базы данных. Объем и важность информации не окупают стоимости создания физического сетевого соединения, поэтому для соединения двух сетей используется модем.

Рисунок 6. Подключение сети филиала компании к основной сети с помощью модема

Способ устранения

Подключить одну локальную сеть к другой можно с помощью соединения PPP между двумя системами, как это показано на рисунке. Инициатором соединения должен стать сервер в удаленном офисе. Для этого необходимо настроить профайл исходящего соединения в удаленной системе и профайл входящего соединения в системе в центральном офисе.

Если PC в удаленном офисе нужно предоставить доступ к корпоративной локальной сети (192.168.1.0), то включите пересылку IP в профайле входящего соединения сервера основной сети и настройте маршрутизацию IP для этих PC (в данном примере 192.168.2, 192.168.3, 192.168.1.6, и 192.168.1.5). Также необходимо включить пересылку IP для стека TCP/IP. Это позволит двум локальным сетям TCP/IP обмениваться пакетами. Следует обратить внимание на защиту локальных сетей и настройку DNS для правильного преобразования имен хостов.

Пример конфигурации

Для настройки примера конфигурации в System i Navigator выполните следующие действия:

1. Настройте профайл исходящего соединения в удаленной системе в офисе.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: Коммутируемая линия
   - **Режим работы**: Набор номера
   - **Конфигурация линии связи**: В зависимости от применяемой среды, это может быть отдельная линия или пул линий.
2. На странице Общие страницы свойств нового профайла PPP введите имя и описание профайла исходящего соединения PPP.
3. Нажмите кнопку **Соединение**, чтобы открыть страницу Соединение. Выберите соответствующее имя линии или введите новое имя с помощью кнопки **Создать**.
   a. На странице Общие выделите существующий аппаратный ресурс и присвойте параметру Обработка кадров значение **Асинхронная**.
   b. Нажмите кнопку **Модем**, чтобы открыть страницу Модем. В списке имен модемов выберите имя применяемого модема.
   c. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
4. Для установления соединения с системой в центральном офисе нажмите кнопку **Добавить** и введите номер телефона. Убедитесь в том, что номер введен с правильными префиксами.
5. Нажмите кнопку **Идентификация**, чтобы открыть станицу Идентификация, и выберите опцию **Разрешить удаленной системе идентификацию сервера iSeries**. Выберите опцию **Запрашивать зашифрованный пароль (CHAP-MD5)** и введите требуемое имя пользователя и пароль.
6. Нажмите кнопку **Параметры TCP/IP**, чтобы открыть страницу параметров TCP/IP.
   a. В качестве локального IP-адреса выберите IP-адрес интерфейса удаленной локальной сети (192.168.2.1) в окне **Применять фиксированный IP-адрес**.
   b. Для удаленного IP-адреса выберите **Назначается удаленной системой**.
   c. В разделе маршрутизации выберите опцию **Добавить удаленную систему в маршрут по умолчанию**.
   d. Нажмите **OK** для создания профайла исходящего соединения.
7. Настройте профайл входящего соединения в системе в центральном офисе.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: Коммутируемая линия
   - **Режим работы**: Ответ

- **Конфигурация линии связи**: В зависимости от применяемой среды, это может быть отдельная линия или пул линий.

8. На странице Общие страницы свойств нового профайла PPP введите имя и описание профайла входящего соединения PPP.
9. Нажмите кнопку **Соединение**, чтобы открыть страницу Соединение. Выберите соответствующее имя линии или введите новое имя с помощью кнопки **Создать**.
   a. На странице Общие выберите существующий аппаратный ресурс и присвойте параметру Обработка кадров значение **Асинхронная**.
   b. Нажмите кнопку **Модем**, чтобы открыть страницу Модем. В списке имен модемов выберите имя применяемого модема.
   c. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
10. Нажмите кнопку **Идентификация**, чтобы открыть страницу Идентификация.
    a. Выберите **Обязательная проверка и идентификация удаленных систем сервером iSeries**.
    b. Добавьте нового удаленного пользователя в контрольный список.
    c. Задайте обязательную идентификацию CHAP-MD5.
11. Нажмите кнопку **Параметры TCP/IP**, чтобы открыть страницу параметров TCP/IP.
    a. В качестве локального IP-адреса укажите IP-адрес интерфейса сервера в центральном офисе (192.168.1.1), выбрав его в поле **выбор**.
    b. Для удаленного IP-адреса укажите **Выбирается в зависимости от ИД пользователя удаленной системы**.Появится окно диалога **IP-адреса, определяемые именем пользователя**. Нажмите **Добавить**. Введите информацию в полях ИД инициатора, IP-адрес и Маска подсети. Для нашего сценария эта информация будет следующей:
       - ИД инициатора: Удаленное_расположение
       - IP-адрес: 192.168.2.1
       - Маска подсети: 255.255.255.0

       Нажмите **OK**, затем еще раз нажмите **OK** для возврата к странице настроек TCP/IP.
    c. Для того чтобы системы в сети могли использовать систему в качестве шлюза, необходимо выбрать опцию **Пересылка IP**.
12. Нажмите **OK** для создания профайла входящего соединения.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Ссылки, связанные с данной

“Конфигурация линии связи” на стр. 52
Конфигурация линии связи задает тип линии, применяемый для создания соединения PPP.

“Пул линий” на стр. 53
Выберите этот тип для создания соединения PPP с применением линии из пула линий. При создании соединения PPP система выбирает из пула незанятую линию. Для профайлов набора номера по запросу линия не выбирается до тех пор, пока система не обнаружит пакеты TCP/IP, которые необходимо отправить удаленной системе.

Сценарий: Идентификация коммутируемых соединений с помощью Сервера сетевого доступа (NAS) RADIUS

Сервер сетевого доступа (NAS), запущенный в системе может направлять запрос на идентификацию от входящих клиентов на отдельный сервер Службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS). После идентификации сервер RADIUS может управлять IP-адресами пользователей.

Ситуация

Удаленные пользователи подключаются по коммутируемому соединению к корпоративной сети через две системы. Вы хотите выполнять идентификацию, обслуживание и учет централизованно, чтобы одна система обрабатывал запросы на проверку ИД и паролей пользователей и определял их IP-адреса.

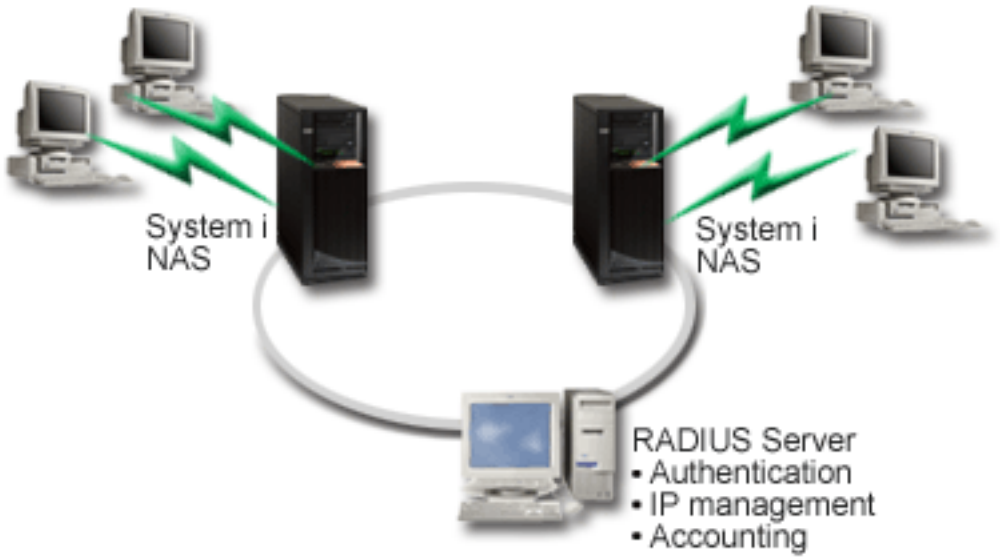


Рисунок 7. Идентификация коммутируемых соединений с помощью сервера RADIUS

Способ устранения

Когда пользователь отправляет запрос на подключение, NAS, запущенный в системе пересылает идентификационную информацию сетевому серверу RADIUS. Сервер RADIUS, обслуживающий все запросы на идентификацию в сети, обрабатывает данный запрос и отсылает ответ. Если пользователь пройдет проверку, то сервер RADIUS может также присвоить ему IP-адрес узла и начать отслеживать его деятельность. Для поддержки службы RADIUS необходимо определить сервер NAS RADIUS в системе.

Пример конфигурации

Для настройки примера конфигурации в System i Navigator выполните следующие действия:

1. В System i Navigator выберите **Сеть**, щелкните правой кнопкой на **Службах удаленного доступа** и выберите **Службы**.
2. На вкладке **RADIUS** выберите **Включить соединения Сервера сетевого доступа RADIUS** и **Включить идентификацию с помощью RADIUS**. В зависимости от конфигурации RADIUS, вы можете также выбрать ведение учета соединений и настройку IP-адресов с помощью RADIUS.
3. Нажмите кнопку **Параметры NAS RADIUS**.
4. На странице Общие введите описание сервера.
5. На странице Сервер идентификации (и, возможно, Сервер учета) нажмите кнопку **Добавить** и введите следующую информацию:
   a. В поле **Локальный IP-адрес** введите IP-адрес интерфейса, через который подключен сервер RADIUS.
   b. В поле **IP-адрес сервера** введите IP-адрес сервера RADIUS.
   c. В поле **Пароль** введите пароль, по которому система идентифицирует себя на сервере RADIUS.

d. В поле **Порт** введите порт системы, через который подключен сервер RADIUS. По умолчанию сервер идентификации подключен к порту 1812, а сервер учета - к порту 1813.

6. Нажмите **OK**.
7. В System i Navigator разверните список **Сеть → Службы удаленного доступа**.
8. Выберите профайл соединения, применяющий сервер RADIUS для идентификации. Службы RADIUS применимы только для профайлов входящих соединений.
9. На странице Идентификация выберите **Обязательная проверка и идентификация удаленных систем**.
10. Выберите **Удаленная идентификация с помощью сервера RADIUS**.
11. Выберите протокол идентификации (PAP или CHAP-MD5). Этот протокол также должен применяться сервером RADIUS.
12. Выберите пункт **Применять RADIUS для изменения и учета соединений**.
13. Нажмите **OK** для сохранения изменений в профайле соединения.

Вы должны также настроить сервер RADIUS, включая поддержку протокола идентификации, пользовательских данных, паролей и учетной информации. За дополнительной информацией обратитесь к поставщику RADIUS.

При подключении пользователей с помощью данного профайла система перешлет идентификационную информацию указанному серверу RADIUS. Если пользователь пройдет проверку, то соединение будет установлено и к нему будут применены все ограничения, указанные для данного пользователя на сервере RADIUS.

Задачи, связанные с данной

“Включение служб RADIUS и DHCP для профайлов соединений” на стр. 63
Здесь приведены действия по включению RADIUS или служб Протокола динамической настройки хостов (DHCP) для профайлов входящих соединений PPP.

Ссылки, связанные с данной

“Идентификация систем” на стр. 45
Соединения PPP с платформой System i предусматривают несколько вариантов идентификации как удаленных клиентов, подключающихся к системе, так и соединений с провайдером Internet (ISP) или с другим сервером, к которому система.

“Обзор службы дистанционной аутентификации пользователей по коммутируемым линиям” на стр. 46
Служба RADIUS - это протокол Internet, который позволяет применять центральный сервер для идентификации, ведения учетных записей и обслуживания удаленных пользователей в распределенной модемной сети.

Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов

Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Ситуация

В вашей сети находятся несколько групп распределенных пользователей, каждой из которых необходим доступ к различным ресурсам корпоративной локальной сети. Группе пользователей, работающих с записями данных, необходим доступ к базе данных и некоторым другим приложениям. Деловому партнеру необходим коммутируемый доступ к службам HTTP, FTP и Telnet, причем по соображениям безопасности ему нельзя предоставить доступ к другим службам или потоку TCP/IP. Определение атрибутов соединений и прав доступа для каждого пользователя слишком утомительно, а определение сетевых ограничений одновременно для всех пользователей данного профайла соединения не обеспечит нужного уровня контроля.

По этой причине, вы хотите определить параметры для нескольких групп пользователей, обычно подключающихся к системе.

Рисунок 8. Применение параметров соединения к коммутируемым соединениям на основе групповых стратегий

Способ устранения

Необходимо применить уникальные параметры фильтрации IP-пакетов к двум разным группам пользователей. Для этого необходимо создать групповые стратегии доступа и правила фильтрации IP-пакетов. Поскольку групповые стратегии доступа ссылаются на правила фильтрации IP-пакетов, сначала следует создать правила. В этом примере необходимо создать фильтр PPP с правилами фильтрации IP-пакетов, предназначенный для групповой стратегии доступа Деловой партнер IBM. Эти правила фильтрации разрешат доступ к службам HTTP, FTP и Telnet, но запретят доступ ко всем прочим службам и данным TCP/IP через систему. Этот сценарий содержит правила фильтрации только для данной группы; однако вы можете задать аналогичные правила фильтрации и для группы Записи данных.

Наконец, необходимо создать групповые стратегии (по одной на каждую группу) для определения групп. Групповые стратеги доступа позволяют определить общие атрибуты соединения для всех пользователей, входящих в группу. После добавления Групповой стратегии доступа в Контрольный список системы вы можете задать эти параметры соединений в процессе идентификации. Групповая стратегия доступа указывает некоторые параметры пользовательских сеансов, например, возможность применения правил фильтрации IP-пакетов для запрета IP-адресов и перечень служб TCP/IP, доступных пользователю во время сеанса.

Пример конфигурации

Для настройки примера конфигурации в System i Navigator выполните следующие действия:

1. Создайте идентификатор фильтра PPP и правила фильтрации IP-пакетов для данной групповой стратегии доступа.
   a. В System i Navigator разверните список **Сеть → Службы удаленного доступа**.
   b. Откройте **Профайлы входящих соединений** и выберите Стратегии группового доступа.
   c. Щелкните правой кнопкой мыши на одной из заранее созданных групп, показанных в правой панели, и выберите **Свойства**.

      Примечание: Для того чтобы создать новую стратегию группового доступа, щелкните правой кнопкой на пункте **Стратегии группового доступа** и выберите **Создать стратегию**

группового доступа. Заполните необходимую информацию на вкладке **Общие**. После этого откройте вкладку **Параметры TCP/IP** и перейдите к этапу e, описанному ниже.

d. Выберите вкладку **Параметры TCP/IP** и нажмите **Дополнительно**.

e. Выберите пункт **Применять фильтрацию IP-пакетов в этом соединении** и нажмите кнопку **Изменить файл правил**.Будет запущен Редактор правил обработки IP-пакетов, в окне которого будет открыт файл фильтра PPP.

f. Откройте меню **Вставка** и выберите **Фильтры** для добавления набора фильтров.Вкладка **Общие** служит для определения наборов правил,а вкладка **Службы** - для определения разрешаемой службы, например HTTP. Следующий набор фильтров, ″services_rules,″ разрешает работу со службами HTTP, FTP и Telnet. Правила фильтрации включают неявное правило запрета по умолчанию, запрещающее работу с любыми службами TCP/IP и потоками данных IP, кроме тех, которые разрешены явно.

Примечание: IP-адреса в следующем примере являются доступными из Internet и приведены только для примера.

```
###Следующие 2 фильтра разрешают работу с входящим и
исходящим потоками данных HTTP (Web-браузер).

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

###Следующие 4 фильтра разрешают работу с входящим и
исходящим потоками данных FTP.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF
###Следующие 2 фильтра разрешают работу с входящим и
исходящим потоками данных Telnet.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

g. Откройте меню **Вставка** и выберите **Интерфейс фильтра**. Интерфейс фильтра позволит создать идентификатор фильтра PPP и связать с ним определенные ранее наборы фильтров.

   1) На вкладке **Общие** укажите `permitted_services` в качестве идентификатора фильтра PPP.

   2) На вкладке **Наборы фильтров** выберите набор фильтров **services_rules** и нажмите **Добавить**.

   3) Нажмите OK. В файл правил будет добавлена следующая строка:

```
###Следующий оператор связывает набор фильтров
'services_rules' с
ИД фильтра PPP "permitted_services."
```

```
Этот ИД фильтра PPP
затем может быть применен к физическому
интерфейсу, связанному с профайлом соединения PPP
или
Групповой стратегией доступа.

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

h. Сохраните изменения и закройте меню. Если впоследствии эти изменения потребуется отменить, введите в текстовом интерфейсе следующую команду RMVTCPTBL *ALL. Эта команда удалит все правила фильтрации и NAT (Преобразование сетевых адресов) в системе.

i. В окне диалога **Дополнительные параметры TCP/IP** оставьте поле **Идентификатор фильтра PPP** пустым и нажмите кнопку **OK** для выхода из меню. Впоследствии вы должны будете применить созданный идентификатор фильтра к Групповой стратегии доступа, а не к профайлу соединения.

2. Определите новую групповую стратегию доступа для этой группы пользователей.
   a. В System i Navigator откройте раздел **Сеть → Службы удаленного доступа → Профайлы входящих соединений**.
   b. Щелкните правой кнопкой мыши на значке **Групповые стратегии доступа** и выберите **Создать групповую стратегию доступа**. System i Navigator перейдет к окну диалога **Создать групповую стратегию доступа**.
   c. На странице Общие введите имя и описание Групповой стратеги доступа.
   d. На странице Параметры TCP/IP выполните следующие действия:
      - Выберите **Применять фильтрацию IP-пакетов** и укажите идентификатор фильтра PPP **permitted_services**.
   e. Выберите **OK** для сохранения Групповой стратеги доступа.
3. Примените групповую стратегию доступа к пользователям, связанным с данной группой.
   a. Откройте профайл входящих соединений, управляющий этими соединениями по телефонной линии.
   b. На странице Идентификация профайла входящих соединений выберите контрольный список, содержащий идентификационную информацию пользователей, и нажмите кнопку **Открыть**.
   c. В группе продаж выберите пользователя, к которому вы хотите применить групповую стратегию доступа, и нажмите **Открыть**.
   d. Нажмите **Применить групповую стратегию к пользователю** и выберите Групповую стратегию доступа, определенную на шаге 2.
   e. Повторите операцию для всех пользователей из этой группы.

Понятия, связанные с данным

“Настройка групповой стратегии доступа” на стр. 61
Папка **Групповые стратегии доступа** раздела Профайлы входящих соединений позволяет настраивать параметры двухточечных соединений для групп удаленных пользователей. Они применяются только для соединений, инициированных удаленной системой, и принятых локальной системой.

“Поддержка групповых стратегий” на стр. 4
Используя поддержку групповых стратегий, администратор сети может определять пользовательские групповые стратегии для управления ресурсами. Индивидуальным пользователям можно назначать стратегии контроля доступа при входе по протоколу PPP или L2TP.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

“Применение правил фильтрации IP-пакетов в соединениях PPP” на стр. 62
С помощью файла правил фильтрации пакетов можно ограничить доступ пользователя или группы к IP-адресам в локальной сети.

Ссылки, связанные с данной

“Контрольный список” на стр. 47
В контрольном списке хранятся ИД и пароли удаленных пользователей.

“Идентификация систем” на стр. 45
Соединения PPP с платформой System i предусматривают несколько вариантов идентификации как удаленных клиентов, подключающихся к системе, так и соединений с провайдером Internet (ISP) или с другим сервером, к которому система.

Информация, связанная с данной

Фильтрация IP-пакетов и преобразование сетевых адресов

Сценарий: Применение общего модема в разных логических разделах с помощью протокола L2TP

В этом примере четыре логических раздела объединены в виртуальную сеть Ethernet. Данный сценарий позволяет применять в нескольких разделах один общий модем для подключения к внешней сети.

Ситуация

Вы являетесь системным администратором компании среднего размера. У вас возникла необходимость обновить компьютерное оборудование, но вы решили расширить модернизацию, и объединить все аппаратное обеспечение в единую систему. Этот процесс начинается с переноса задач с трех старых систем в одну новую. В системе были созданы три логических раздела. Новая система поставляется с внутренним модемом 2793. Данный модем является единственным процессором ввода-вывода (IOP) системы, который поддерживает PPP. Также есть старый модем электронной поддержки заказчиков (ECS) 7852–400.

Способ устранения

Несколько систем и разделов могут устанавливать телефонные соединения с помощью одного модема, что позволяет не приобретать отдельный модем для каждого раздела. Это возможно при применении туннелей L2TP и настройке профайлов L2TP для внешних вызовов. В локальной сети туннели создаются на основе виртуальной сети Ethernet и физической сети. Физическая линия соединяет с другой системой, использующей модемы в сети.

Сведения

На следующем рисунке проиллюстрирована рассматриваемая в данном сценарии сеть:

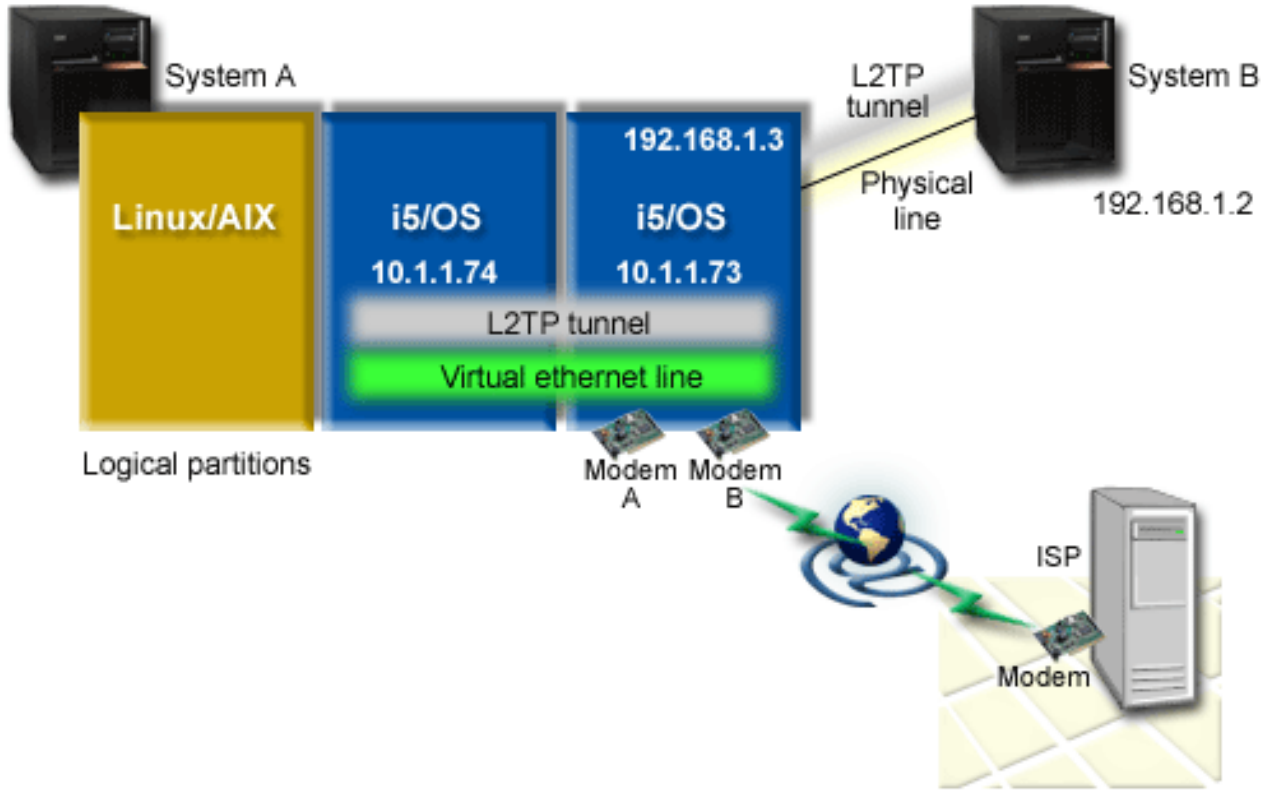


Рисунок 9. Несколько систем используют общий модем для установления телефонных соединений

Предварительные требования и предположения

System A должна соответствовать следующим требованиям настройки:

- В разделе, в котором расположены модемы с поддержкой асинхронных соединений (ASYNC), должна быть установлена ОС i5/OS версии 5, выпуска 3 или более позднего выпуска.
- Аппаратное обеспечение, позволяющее создавать в системе логические разделы.
- System i Access for Windows иSystem i Navigator (компонент Настройка и обслуживание System i Navigator) Версия 5 выпуск 3 или выше.
- В системе создано не менее двух логических разделов (LPAR). В разделе, в котором расположен модем, должна быть установлена система i5/OS версии 5, выпуска 3 или более позднего выпуска. В остальных разделах могут быть установлены операционные системы OS/400 V5R2, i5/OS V5R3, Linux или AIX. В данном сценарии разделы работают под управлением системы i5/OS или the Linux.
- Для обмена данными между разделами создана виртуальная сеть Ethernet.

System B должна иметь установленные лицензионную программу и соответствующие компоненты System i Navigator: System i Access for Windows иSystem i Navigator (компонент Настройка и обслуживание System i Navigator) версии 5 выпуска 2 или выше.

Информация, связанная с данной

Логические разделы

Детали сценария: Применение общего модема в разных логических разделах с помощью протокола L2TP

После проверки выполнения предварительных требований можно начать настройку профайлов L2TP.

Этап 1: Настройка профайла терминатора L2TP для любого интерфейса раздела, в котором расположены модемы:

Для создания профайла вызываемой стороны для любого интерфейса выполните следующие действия:

1. В System i Navigator разверните ***ваша система*** → **Сеть** → **Служба удаленного доступа**.
2. Щелкните правой кнопкой мыши на значке **Профайлы входящих соединений** и выберите опцию **Создать профайл**.
3. На странице Настройка задайте значения следующих параметров и нажмите **OK**:
   - **Тип протокола**: PPP
   - **Тип соединения**: L2TP (виртуальная линия)
   - **Режим работы**: Терминатор (сетевой сервер)
   - **Тип физической линии**: Отдельная линия
4. На вкладке **Создание профайла - Общие** задайте значения в следующих полях:
   - **Имя**: toExternal
   - **Описание**: Соединение для исходящих вызовов
   - Выберите **Запускать профайл с TCP**.
5. На вкладке **Создание профайла - Соединение** задайте значения в следующих полях.
   - **IP-адрес конечной точки локального туннеля**: ANY
   - **Имя виртуальной линии**: toExternal.С этой линией не связаны физические интерфейсы. Описание виртуальной линии содержит различные параметры данного профайла PPP. После открытия окна Свойства линии L2TP щелкните на вкладке **Идентификация** и введите имя хоста системы. Нажмите **OK** для возврата на вкладку **Соединение** окна Свойства нового профайла PPP.
6. Выберите **Разрешить исходящие соединения**. На экране появится окно диалога **Свойства исходящего соединения**.
7. В окне Свойства исходящего соединения выберите тип физической линии.
   - **Тип физической линии**: Пул линий
   - **Имя**: dialOut
   - Нажмите кнопку **Создать**.На экране появится окно **Свойства нового пула линий**.
8. Выберите в этом окне линии и модемы, для которых будут разрешены исходящие вызовы, и нажмите кнопку **Добавить**. Если эти лини необходимо определить, выберите опцию **Создать линию**.Интерфейсы раздела, в котором расположены модемы, попытаются использовать любую свободную линию из данного пула линий. На экране появится окно свойств новой линии.
9. На вкладке **Свойства новой линии - Общие** заполните следующие поля:
   - **Имя**: line1
   - **Описание**: Первая линия и первый модем для пула линий (внутренний модем 2793)
   - **Аппаратный ресурс**: cmn03 (порт связи)
10. На всех остальных вкладках примите значения по умолчанию и нажмите **OK** для возврата к окну Свойства нового пула линий.
11. В окне Свойства нового пула линий выберите линии и модемы, для которых будут разрешены исходящие вызовы, и нажмите кнопку **Добавить**. Убедитесь в том, что для пула выбран модем 2793.
12. Еще раз нажмите кнопку **Создать линию** и добавьте модем Электронной поддержки заказчиков (ECS) 7852–400. На экране появится окно свойств новой линии.
13. На вкладке **Свойства новой линии - Общие** заполните следующие поля:
    - **Имя**: line2
    - **Описание**: вторая линия и второй модем пула линий (внешний модем Электронной поддержки заказчиков (ECS) 7852-400)
    - **Аппаратный ресурс**: cmn04 (порт V.24)
    - **Обработка кадров**: Асинхронная
14. На вкладке **Свойства новой линии - Модем** выберите внешний модем (7852–400) и нажмите **OK** для возврата к окну Свойства нового пула линий.

15. Выберите все доступные линии, которые следует добавить в пул линий, и нажмите кнопку **Добавить**.В данном примере следует убедиться, что два новых модема, добавленных в список, указаны в поле **Выбранные линии пула линий**. Нажмите кнопку **OK** для возврата к окну Свойства исходящего соединения.
16. В окне Свойства исходящего соединения введите Номер для набора по умолчанию и нажмите **OK** для возврата к окну Свойства нового профайла PPP.

    Примечание: Этим номером может служить номер ISP, на который будут часто звонить другие системы, использующие данный модем. Если в других системах задан номер телефона *PRIMARY или *BACKUP, то набираться будет номер, указанный в этом поле. Если в других системах будет задан фактический номер телефона, то набираться будет он.
17. На вкладке **Параметры TCP/IP** задайте следующие значения:
    - **Локальный IP-адрес**: Нет
    - **Удаленный IP-адрес**: Нет

    Примечание: Если требуется использовать профайл для завершения сеанса L2TP, необходимо выбрать локальный IP-адрес, соответствующий системе. Для удаленных IP-адресов необходимо выбрать пул адресов, принадлежащий подсети системы. IP-адреса для всех сеансов L2TP будут выделяться из этого пула.
18. На вкладке **Идентификация** примите все значения по умолчанию.

Настройка профайла терминатора L2TP в разделе с модемами завершена. Теперь необходимо настроить удаленный профайл исходящего соединения L2TP для интерфейса 10.1.1.74.

Ссылки, связанные с данной

“Профайл с поддержкой нескольких соединений” на стр. 54
Профайл PPP с поддержкой нескольких соединений позволяет использовать один профайл для обслуживания нескольких вызовов по аналоговым или цифровым линиям, а также туннелям L2TP.

Этап 2: Настройка профайла исходящего соединения L2TP для интерфейса 10.1.1.74:

Выполните данные действия для создания профайла исходящего соединения L2TP.

1. В System i Navigator разверните**10.1.1.74 → Сеть → Служба удаленного доступа**.
2. Щелкните правой кнопкой мыши на значке **Профайлы исходящих соединений** и выберите опцию **Создать профайл**.
3. На странице Настройка задайте значения следующих параметров и нажмите **OK**:
   - **Тип протокола**: PPP
   - **Тип соединения**: L2TP (виртуальная линия)
   - **Режим работы**: Удаленный набор номера
   - **Тип физической линии**: Отдельная линия
4. На вкладке **Общие** задайте значения в следующих полях:
   - **Имя**: toModem
   - **Описание**: исходящее соединение с разделом, в котором расположен модем
5. На вкладке **Соединение** задайте значения в следующих полях:

   Имя виртуальной линии: toModem. С этой линией не связан физический интерфейс. Описание виртуальной линии содержит различные параметры данного профайла PPP. На экране появится окно свойств линии L2TP.
6. На вкладке **Общие** задайте имя и описание виртуальной линии.
7. На вкладке **Идентификация** укажите имя локального хоста раздела и нажмите **OK** для возврата на страницу Соединение.

8. В поле **Номера удаленных телефонов** укажите значения *PRIMARY и *BACKUP. В этом случае при создании соединения будет набираться номер, указанный в профайле терминатора в разделе, в котором расположены модемы.
9. В поле **IP-адрес или имя хоста хоста конечной точки удаленного туннеля** укажите IP-адрес конечной точки удаленного туннеля(10.1.1.73).
10. На вкладке **Идентификация** выберите значение **Разрешить удаленной системе идентификацию сервера iSeries**.
11. В поле Протокол идентификации выберите **Обязательное шифрование паролей (CHAP-MD5)**. По умолчанию выбрано также **Разрешить протокол гибкой идентификации**.

    Примечание: Выбранный протокол должен соответствовать протоколу, применяемому в системе.
12. Введите имя пользователя и пароль.

    Примечание: Имя пользователя и пароль должны совпадать с правильными именем пользователя и паролем, заданными в системе.
13. Откройте вкладку **Параметры TCP/IP** и проверьте правильность следующих значений:
    - **Локальный IP-адрес**: Задается удаленной системой
    - **Удаленный IP-адрес**: Задается удаленной системой
    - **Маршрутизация**: Дополнительная маршрутизация не требуется
14. Нажмите **OK** для сохранения изменений в профайле PPP.

Этап 3: Настройка профайла удаленного набора номера L2TP для интерфейса 192.168.1.2:

Можно настроить профайл удаленного набора номера L2TP для 192.168.1.2, повторив шаг 2 и указав в качестве адреса конечной точки удаленного туннеля 192.168.1.3 ((физический интерфейс, к которому подключается System B).

Примечание: Указанные IP-адреса не используются в действительности и служат только в качестве примеров.

Этап 4: Проверка работы соединения:

После завершения настройки обоих систем необходимо проверить работу соединений, убедившись в том, что системы могут использовать общий модем для подключения к удаленным сетям.

1. Убедитесь в том, что профайл L2TP вызываемой стороны активен.
   a. В System i Navigator откройте раздел **10.1.1.73 → Сеть → Службы удаленного доступа → Профайлы входящих соединений**.
   b. На правой панели найдите нужный профайл (toExternal) и убедитесь в том, что в поле **Состояние** указано значение Активный. Если это не так, щелкните правой кнопкой мыши на профайле и выберите опцию **Запуск**.
2. Запустите профайл удаленного набора номера интерфейса 10.1.1.74.
   a. В System i Navigator откройте раздел **10.1.1.74 → Сеть → Службы удаленного доступа → Профайлы исходящих соединений**.
   b. На правой панели найдите нужный профайл (toModem) и убедитесь в том, что в поле **Состояние** указано значение Активный. Если это не так, щелкните правой кнопкой мыши на профайле и выберите опцию **Запуск**.
3. Запустите профайл удаленного набора номера интерфейса System B.
   a. В System i Navigator откройте раздел **192.168.1.2 → Сеть → Службы удаленного доступа → Профайлы исходящих соединений**.
   b. На правой панели найдите созданный профайл и убедитесь в том, что в поле **Состояние** указано значение Активный. Если это не так, щелкните правой кнопкой мыши на профайле и выберите опцию **Запуск**.

4. Если возможно, проверьте с помощью команды ping соединение с провайдером Internet (ISP) или другим набранным узлом, и убедитесь в том, что оба профайла включены. Необходимо проверить работу соединения с двух интерфейсов - 10.1.1.74 и 192.168.1.2.
5. Работу соединения можно также проверить с помощью окна Состояние соединения.
   a. В System i Navigator откройте раздел **Система → Сеть → Службы удаленного доступа → Профайлы исходящих соединений**.
   b. В правой панели щелкните правой кнопкой мыши на созданном профайле и выберите опцию **Соединения**. В окне Состояние соединения показаны все активные, неактивные, находящиеся в процессе подключения и другие профайлы.

Планирование PPP

Планирование протокола двухточечной связи (PPP) подразумевает создание соединений PPP и администрирование ими.

Ссылки, связанные с данной

“Сценарий: Подключение удаленных клиентов к системе” на стр. 13
Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

“Сценарий: Подключение локальной сети к Internet с помощью модема” на стр. 15
Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Систему можно подключить к ISP с помощью модема. Клиенты PC, подключенные к сети, будут использовать операционную систему i5/OS в качестве шлюза при доступе к Internet.

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Требования к программному и аппаратному обеспечению

Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров - платформа System i, может быть как инициатором, так и обработчиком соединения.

Для обеспечения доступа удаленных систем система должна соответствовать следующим требованиям:

- System i Navigator с поддержкой TCP/IP.
- Один из двух профайлов соединений:
  - Для работы с исходящими соединениями необходим профайл исходящего соединения PPP.
  - Для работы со входящими соединениями необходим профайл входящего соединения PPP.
- Консоль рабочей станции, на которой установлена программа System i Access for Windows 95 или более поздней версии с System i Navigator.
- Установленный адаптер.

  Адаптер можно выбрать из следующего списка:
  - 2699*: WAN IOA на две линии.
  - 2720*: PCI WAN/твинаксиальный IOA.
  - 2721*: PCI WAN IOA на две линии.
  - 2745*: PCI WAN IOA на две линии (замена для IOA 2721).
  - 2742*: IOA на две линии (замена для IOA 2745).
  - 2771: Двухпортовый WAN IOA со встроенным в первый порт модемом V.90 и стандартным интерфейсом соединений для второго порта. Для применения второго порта адаптера 2771 необходим внешний модем или терминальный адаптер ISDN с соответствующим кабелем.
  - 2772: Двухпортовый интегрированный модем V.90 WAN IOA.
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: Адаптер Ethernet для соединений PPPoE.

– 2793/576C*: Двухпортовый WAN IOA со встроенным в первый порт модемом V.92 и стандартным интерфейсом соединений для второго порта. Для применения второго порта необходим внешний модем или терминальный адаптер ISDN с соответствующим кабелем.
– 2805 4-портовый WAN IOA со встроенным аналоговым модемом V.92. Он заменяет модели 2761 и 2772.

* Для применения этих адаптеров необходим внешний модем V.90 (или выше) или терминальный адаптер ISDN и кабель RS-232 (EIA 232) или совместимый с ним.

- В зависимости от типа линии и соединения вам потребуется следующее оборудование:
  – Внешний или внутренний модем или устройство обслуживания канала и обработки данных (CSU/DSU).
  – или терминальный адаптер цифровой сети с комплексными услугами (ISDN).
- Для подключения к Internet необходимо получить учетную запись у провайдера Internet (ISP). Провайдер должен предоставить вам требуемые номера телефонов и информацию о соединении с Internet.

Ссылки, связанные с данной

“Профайлы соединений” на стр. 2
Профайлы двухточечных (PPP) соединений задают набор параметров и ресурсов для конкретного соединения PPP. Эти профайлы можно применять для входящих или для исходящих соединений PPP.

“Модемы” на стр. 40
Для создания соединений PPP применяются как внутренние, так и внешние модемы.

“CSU/DSU” на стр. 40
Устройство обслуживания канала (CSU) - это устройство, соединяющее терминал с цифровой линией. Устройство обслуживания данных (DSU) - это устройство для защиты и диагностики телекоммуникационной линии связи. Обычно эти два устройства объединяются в один блок - CSU/DSU.

“Терминальные адаптеры ISDN” на стр. 40
Цифровая сеть с комплексными услугами (ISDN) обеспечивает цифровое соединение для одновременной передачи речевой, цифровой, видео- и прочей информации в произвольном сочетании.

Альтернативные способы соединения

Протокол двухточечной связи (PPP) может передавать дейтаграммы по последовательным двухточечным линиям связи.

PPP позволяет взаимодействовать оборудованию нескольких производителей и нескольким протоколам с помощью стандартизации двухточечных соединений. На уровне передачи данных PPP применяется обработка кадров HDLC для инкапсулирования дейтаграмм при синхронном и асинхронном методах передачи данных.

Протокол PPP поддерживает несколько типов линий связи, в то время как Протокол подключения к Internet по последовательной линии (SLIP) поддерживает только асинхронные линии связи. SLIP применяется только для аналоговых линий. Телефонные компании как правило предоставляют широкий спектр традиционных телекоммуникационных услуг. Для предоставления этих услуг применяются стандартные линии передачи голоса.

Линии связи PPP устанавливают физическое соединений между локальным и удаленным хостами. Эти линии связи обеспечивают выделенную полосу пропускания. При их реализации применяется широкий спектр протоколов и значений скоростей передачи данных. Линии связи PPP поддерживают соединения следующих типов:

Аналоговые телефонные линии

Одним из самых старых типов линий для двухточечных соединений является аналоговая линия, на основе которой можно создавать выделенные или коммутируемые линии.

Выделенные линии - это постоянные соединения между двумя заданными расположениями, а коммутируемые линии - это стандартные голосовые линии. Скорость передачи несжатых данных по модему в настоящее время не превосходит 56 Кбит/с. Очень часто из-за низкого соотношения сигнал/шум даже эта скорость недостижима.

Производители модемов заявляют о более высоких скоростях модемов, которые обычно достигаются благодаря применению в них алгоритма сжатия данных (CCITT V.42bis). Несмотря на то, что теоретически применение алгоритма V.42bis позволяет увеличить объем передаваемых данных в 4 раза, степень сжатия зависит от типа данных и редко достигает даже 50%. Объем уже сжатых или зашифрованных данных может даже увеличиться при применении этого алгоритма. Алгоритмы X2 или 56Flex позволят увеличить пропускную способность аналоговых телефонных линий до 56 Кбит/с. Это комбинированная технология, для применения которой на одной из сторон соединения PPP должна находиться аналоговая линия, а на другой - цифровая. Кроме того, скорость в 56 Кбит/с достигается только при передаче данных от цифровой линии к аналоговой. Эта технология лучше всего подходит для подключения к провайдеру, оснащенному цифровыми линиями и соответствующим оборудованием. Обычно подключение к аналоговому модему V.24 по последовательному интерфейсу RS-232 с асинхронным протоколом позволяет достигать скорости передачи данных до 115,2 Кбит/с.

После появления стандарта V.90 несовместимость протоколов x2 и K56flex перестала быть актуальной. Стандарт V.90 стал компромиссом двух лагерей в индустрии модемов - x2 и K56flex. При работе с общей коммутируемой телефонной сетью технология V.90 применяет те же методы, что и при работе с цифровой сетью, и это позволяет принимать данные из Internet на скоростях до 56 Кбит/с. Технология V.90 отличается от других стандартов тем, что при ее применении сигнал кодируется цифровым образом, а не модулируется, как при применении аналоговых модемов. Данные передаются в асимметричном режиме, что позволяет отправлять исходящие данные (как правило, сигналы с клавиатуры и мыши, т. е. данные, объем которых сравнительно невелик) центральному сайту на основных скоростях до 33.6 Кбит/с. Данные отправляются модемом в виде аналоговой передачи, соответствующей стандарту V.34. Преимущество технологии V.90 проявляется только при передаче входящих данных.

Стандарт V.92 превосходит стандарт V.90 в скорости передачи исходящих данных, поддерживая значения до 48 Кбит/с. Помимо этого, усовершенствованный процесс квитирования позволяет сократить время соединения, а модемы с функцией блокирования теперь могут оставаться подключенными, когда линия принимает звонок или ожидает звонка.

Цифровая служба и Служба цифровых данных

С PPP можно использовать цифровые службы и Служба цифровых данных (DDS).

Цифровая служба

При цифровой передаче данные передаются от компьютера отправителя в центральный офис телефонной компании, междугородному провайдеру, в центральный офис, а затем компьютеру получателя в цифровом виде. Цифровая передача данных позволяет заметно повысить пропускную способность и надежность линий связи. Применение этой технологии автоматически устраняет многие проблемы, возникающие при аналоговых способах передачи данных, такие как шум, непостоянное качество линий связи и затухание сигнала.

Служба цифровых данных

Основой цифровых служб передачи данных является DDS. DDS работает на выделенных постоянных линиях связи и с постоянными скоростями, достигающими 56 Кбит/с. Эта служба также известна как DS0.

Соединение с DDS можно настроить с помощью специального окна *Устройство обслуживания канала и обработки данных (CSU/DSU)*, соответствующего окну модема в аналоговой схеме. Физические ограничения DDS прямо пропорциональны расстоянию между устройством CSU/DSU и центральным офисом телефонной компании. Рекомендуется применять DDS на дистанции не более 9 километров. Дистанцию можно увеличить с помощью усилителей сигнала, но это приведет к увеличению стоимости передачи

данных. DDS предназначен для соединения двух компьютеров, обслуживаемых одним и тем же центральным офисом. Применение DDS для соединения центральных офисов, расположенных далеко друг от друга, будет невыгодным из-за необходимости усиления сигнала. В этих случаях линия Switched 56 может быть лучшим решением. Обычно подключение к DDS CSU/DSU с помощью последовательного интерфейса V.35, RS449 или X.21 и синхронного протокола позволяет передавать данные на скоростях до 56 Кбит/с.

Ссылки, связанные с данной

"CSU/DSU" на стр. 40
Устройство обслуживания канала (CSU) - это устройство, соединяющее терминал с цифровой линией. Устройство обслуживания данных (DSU) - это устройство для защиты и диагностики телекоммуникационной линии связи. Обычно эти два устройства объединяются в один блок - CSU/DSU.

"Коммутируемые линии-56"
При отсутствии необходимости в постоянном соединении линии типа *Коммутируемая линия-56 (SW56)* могут быть оптимальным вариантом.

Коммутируемые линии-56

При отсутствии необходимости в постоянном соединении линии типа *Коммутируемая линия-56 (SW56)* могут быть оптимальным вариантом.

Работа линии связи SW56 схожа с процессом настройки линии DDS при подключении терминального оборудования к цифровой службе аналогично устройству обработки канала/данных CSU/DSU. Тем не менее, при работе с линией SW56 CSU/DSU необходимо ввести телефонный номер удаленного хоста. SW56 позволяет устанавливать цифровые модемные соединения с любым абонентом SW56 в любой точке земного шара.

Вызов SW56 передается по цифровой сети на большие расстояния так же, как и оцифрованный голосовой вызов. SW56 применяет те же номера телефонов локальной телефонной системы, что и при обычных голосовых вызовах, поэтому стоимость соединений не отличается от стоимости разговоров.

SW56 применяется только в сетях США и Канады и поддерживает только один канал для передачи данных. SW56 является альтернативным соединением для тех случаев, когда применение ISDN невозможно.

Обычно подключение к SW56 CSU/DSU с помощью последовательного интерфейса V.35 или RS 449 позволяет передавать данные на скоростях до 56 Кбит/с. При применении блока вызова/ответа V.25bis управление вызовами и передачей данных возможно с помощью одного последовательного интерфейса.

Ссылки, связанные с данной

"Цифровая служба и Служба цифровых данных" на стр. 34
С PPP можно использовать цифровые службы и Служба цифровых данных (DDS).

"Цифровая сеть с комплексными услугами"
Сеть ISDN обеспечивает цифровую коммутируемую связь. По линиям ISDN можно одновременно передавать как данные, так и голосовую информацию.

Цифровая сеть с комплексными услугами

Сеть ISDN обеспечивает цифровую коммутируемую связь. По линиям ISDN можно одновременно передавать как данные, так и голосовую информацию.

Среди нескольких типов служб ISDN основным является интерфейс BRI. BRI состоит из двух B-каналов с пропускной способностью 64 Кбит/с, предназначенных для передачи данных, и одного D-канала для передачи служебной информации. Для получения пропускной способности 128 Кбит/с два B-канала можно объединить в один. В некоторых районах телефонные компании могут ограничить пропускную способность каждого B-канала значением 56 Кбит/с, что соответствует объединенной пропускной способности в 112 Кбит/с. Кроме того, расстояние от заказчика до коммутатора не должно превышать 5,5 километров. Это расстояние можно увеличить с помощью усилителей. К линии ISDN можно подключиться с помощью терминального адаптера. В большинство терминальных адаптеров встроен сетевой терминал 1, позволяющий напрямую подключать адаптер к телефонной линии. Как правило, большинство терминальных адаптеров подключаются к компьютеру с помощью асинхронного соединения RS-232, а для

их настройки и управления применяется тот же набор команд AT, что и для настройки и управления аналоговыми модемами. Для каждого терминального адаптера существуют свои расширения команд AT, предназначенные для настройки уникальных параметров ISDN. Ранее проблема взаимодействия терминальных адаптеров ISDN разных изготовителей стояла очень остро. Эти проблемы были вызваны в основном наличием большого числа скоростных протоколов, поддерживаемых версиями V.110 и V.120 и схемами объединения двух B-каналов.

В настоящее время для объединения двух B-каналов чаще всего применяется синхронный многоканальный протокол PPP. Некоторые производители терминальных адаптеров встраивают в них поддержку V.34 (аналоговых модемов). Это позволяет клиентам с одной линией ISDN одновременно передавать данные и голос по линиям ISDN для обработки вызовов ISDN или основных аналоговых вызовов. Адаптер терминала, использующий эту технологию, также может работать как сторона цифровой системы для клиентов V.92.

Как правило, подключение к терминальному адаптеру ISDN с помощью последовательного интерфейса RS-232 позволяет передавать данные на скоростях до 230,4 Кбит/с. Тем не менее, скорость передачи данных системой в бодах по асинхронному соединению с интерфейсом RS-232 не может превышать 115,2 Кбит/с. К сожалению, скорость передачи данных ограничена значением 11.5 Кбит/с, в то время как терминальный адаптер с поддержкой нескольких линий позволяет передавать несжатые данные на скорости 14/16 Кбайт/с. Некоторые терминальные адаптеры поддерживают протокол синхронной передачи данных с помощью интерфейса RS-232 на скорости до 128 Кбит/с, однако этот параметр системы ограничен значением 64 Кбит/с.

Система поддерживает протокол асинхронной передачи данных с помощью интерфейса V.35 на скоростях до 230,4 Кбит/с, но терминальные адаптеры, как правило, не поддерживают такой режим. Возможным решением проблемы может стать преобразование интерфейса RS-232 в интерфейс V.35, но эта функция пока не реализована в системе. Кроме того, можно передавать данные с помощью терминальных адаптеров и синхронного протокола V.35 на скорости 128 Кбит/с. Несмотря на то, что такие адаптеры существуют, лишь немногие из них поддерживают синхронную передачу данных по нескольким линиям PPP.

Ссылки, связанные с данной

“Коммутируемые линии-56” на стр. 35
При отсутствии необходимости в постоянном соединении линии типа *Коммутируемая линия-56 (SW56)* могут быть оптимальным вариантом.

“Терминальные адаптеры ISDN” на стр. 40
Цифровая сеть с комплексными услугами (ISDN) обеспечивает цифровое соединение для одновременной передачи речевой, цифровой, видео- и прочей информации в произвольном сочетании.

соединения T1/E1 и раздельный T1

T1/E1 и раздельный T1 являются двумя возможными типами соединения.

T1/E1

Соединение T1 объединяет двадцать четыре разделенных мультиплексных канала (TDM) по 64 Кбит/с (DS0) на одном четырехжильном медном проводе. Общая пропускная способность такого канала составляет 1,544 Мбит/с. Общая пропускная способность канала E1, объединяющего тридцать два таких канала и применяемого в Европе и других странах света, составляет 2,048 Мбит/с. TDM позволяет нескольким пользователям одновременно применять один цифровой канал путем предоставления им выделенных промежутков времени. Многие цифровые PBXs пользуются преимуществами службы T1, позволяющей осуществлять несколько запросов по одной линии T1 вместо того, чтобы проводить 24 отдельных провода между PBX и телефонной компанией.

Очень важно помнить, что канал T1 позволяет одновременно передавать голос и данные. Телефонная компания может применять лишь часть из 24 каналов линии связи T1, зарезервировав остальные, например, для соединения с Internet. Мультиплексор T1 необходим для управления 24 каналами DS0 при разделении канала T1 между несколькими службами. Если по каналу передаются только данные, то линию можно запускать без разделения на каналы. Вместо этого можно использовать более простое устройство CSU/DSU.

Обычно подключение к устройству CSU/DSU с помощью канала T1/E1 или мультиплексора и последовательного интерфейса V.35 или RS 449 и синхронного протокола позволяет передавать данные на скоростях от 64 Кбит/с до 1,544 или 2,048 Мбит/с. Синхронизация в сети выполняется с помощью устройства CSU/DSU или мультиплексора.

Раздельный T1

С помощью раздельного канала T1 (FT1) можно выделять пользователям любое число каналов 64 Кбит/с линии T1. Поэтому FT1 позволяет вести более гибкую ценовую политику в отношении клиентов. Это означает, что клиенты будут платить только за ту полосу пропускания, которая им нужна. Кроме того, канал FT1 позволяет объединять каналы DS0 в центральном офисе телефонной компании, что невозможно при применении единого канала T1. Удаленная сторона канала FT1 находится на цифровом комбинированном коммутаторе, поддерживаемом телефонной компанией. Системы, совместно использующие цифровой коммутатор, могут переключаться между каналами DS0. Эта схема пользуется популярностью среди провайдеров, применяющих один канал T1 для связи с цифровым коммутатором телефонной компании. В этих случаях одна служба FT1 позволяет обслуживать несколько заказчиков. Обычно подключение к устройству CSU/DSU с помощью канала T1/E1 или мультиплексора и последовательного интерфейса V.35 или RS 449 и синхронного протокола позволяет передавать данные на скоростях, кратных 64 Кбит/с. При работе с FT1 заказчику выделяется заранее определенная часть от 24 каналов. Мультиплексор T1 необходимо настроить так, чтобы он занимал только те промежутки времени, которые выделены этой службе.

Frame relay

Frame relay - это протокол, применяющий IP-адрес кадра (идентификатор канала передачи данных) для маршрутизации кадров в сети и управления маршрутом виртуального соединения.

Сети Frame-relay в США поддерживают передачу данных на скоростях T1 (1,544 Мбит/с) и T3 (45 Мбит/с). Протокол frame relay можно представить как способ передачи данных по линиям связи T-1 и T-3, принадлежащим провайдеру. В настоящее время большинство провайдеров предоставляют каналы в сети Fame Relay с пропускной способностью от 56 Кбит/с до T1. (В Европе скорость передачи данных по протоколу Frame Relay колеблется в диапазоне от 64 Кбит/с до 2 Мбит/с. В США этот протокол весьма популярен из-за относительно невысоких тарифов. Тем не менее, в некоторых районах он уже вытесняется более современными технологиями, такими как ATM.)

Поддержка туннелей L2TP для соединений PPP

Туннельный протокол второго уровня (L2TP) - это протокол, расширяющий PPP путем добавления возможности организации туннелей между запрашивающим клиентом L2TP (Концентратором L2TP) и конечной точкой целевого сервера L2TP.

Туннельный протокол второго уровня (L2TP)

С помощью туннелей L2TP можно разделить точки физического подключения к сети и логического доступа к сети. Поэтому L2TP также называется *Виртуальный PPP*.

Эти рисунки иллюстрируют три туннельные реализации L2TP.

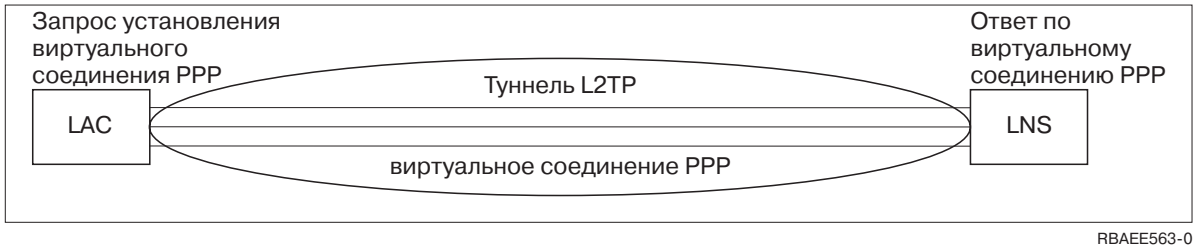


Рисунок 10. Виртуальный вызов PPP или виртуальный ответ PPP

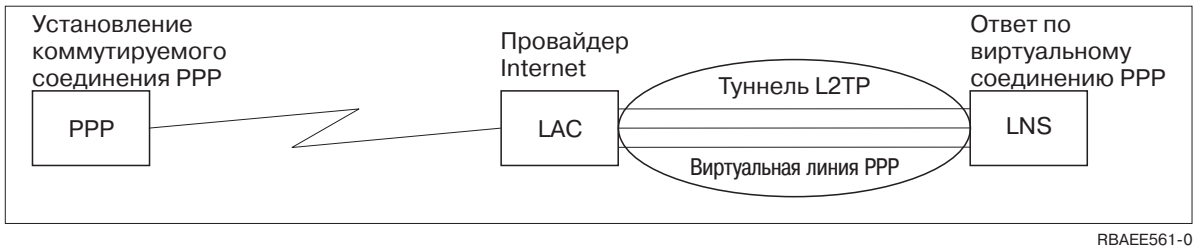


Рисунок 11. Набор номера PPP или виртуальный ответ PPP Virtual Terminator

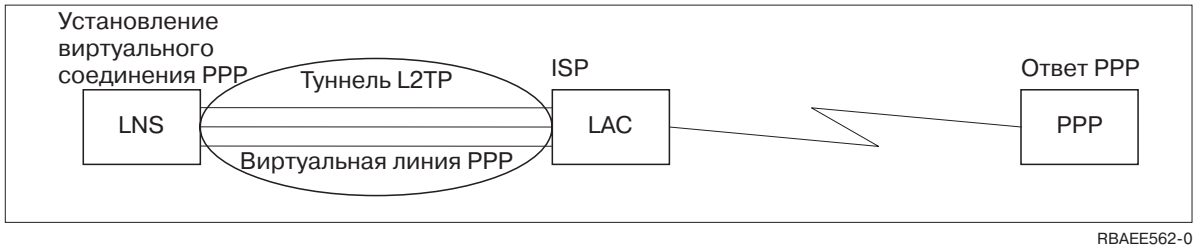


Рисунок 12. Виртуальный набор номера PPP или виртуальный ответ PPP

Протокол L2TP описан в документе RFC-2661. Туннель может относиться ко всему сеансу PPP, либо только к первому сегменту двухсегментного сеанса. Это описывается с помощью четырех различных моделей туннелей.

Информация, связанная с данной

Защита туннеля L2TP с помощью IPSec

Редактор RFC

Дополнительный туннель:

Дополнительный туннель создается пользователем, как правило, с помощью клиента L2TP.

Поэтому пакеты L2TP будут отправляться пользователем ISP и пересылаться на сервер L2TP (LNS). Поддержка дополнительного туннеля L2TP провайдером не обязательна, а инициатор туннеля L2TP может быть размещен в той же системе, что и удаленный клиент. Дополнительный туннель действует для всего сеанса PPP - от клиента L2TP до LNS.

Основной туннель - входящий вызов:

В этой модели туннель создается независимо от пользователя.

В результате пользователь отправляет пакеты по двухточечному протоколу провайдеру Internet (ISP) (Концентратор L2TP (LAC)). Провайдер Internet преобразовывает пакеты в L2TP и посылает их по туннелю на сетевой сервер L2TP (LNS). В этом случае провайдер должен поддерживать протокол L2TP-capable. В этой модели туннель действует только на участке сеанса PPP от провайдера до LNS.

Основной туннель - удаленный набор номера:

В этой модели локальный шлюз (сетевой сервер L2TP (LNS)) создает туннель до провайдера (LAC) и дает ему указание вызвать отвечающего клиента Протокола двухточечной связи (PPP).

Эта модель применима в тех случаях, если у отвечающего клиента PPP есть выделенная телефонная линия, соединяющая его с провайдером. Эта модель предназначена для случаев, когда компании с сайтом в Internet необходимо установить соединение с удаленным офисом по модемной линии связи. В этой модели туннель действует только на участке сеанса PPP от провайдера до LNS.

Транзитное соединение L2TP:

Транзитное соединение L2TP позволяет пересылать поток данных L2TP от имени клиентов Концентратор L2TP (LAC) и сетевых серверов L2TP (LNS).

Транзитное соединение создается с помощью транзитного шлюза L2TP (системы, соединяющей вместе профайлы инициатора и отвечающей стороны L2TP). Для создания транзитного соединения L2TP транзитный шлюз должен выполнять роль как LNS, так и LAC. При этом один туннель создается от клиентского LAC до шлюза, а другой - от шлюза до целевого LNS. Поток данных L2TP от клиентского LAC перенаправляется транзитным шлюзом L2TP на целевой LNS, а поток данных от целевого LNS перенаправляется на клиентский LAC.

Поддержка PPPoE (DSL) для соединений PPP

Под *DSL* понимают технологии, повышающие пропускную способность обычного медного телефонного кабеля, соединяющего клиента и провайдера Internet (ISP).

Технология DSL позволяет одновременно и на высокой скорости передавать голосовую информацию и данные по обычной паре телефонных проводов. Хотя за последнее время быстродействие модемов и возросло за счет использования различных способов сжатия и других технологий, сегодня уже практически достигнут теоретический предел - 56 Кбит/с. Технология DSL обеспечивает гораздо большую скорость передачи информации по витой паре (до 2 Мбит). Двухточечный протокол (PPP) обычно применяется для последовательных соединений, таких как коммутируемые соединения через модем. Многие провайдеры DSL Internet теперь применяют PPP по Ethernet (PPPoE) из-за предусмотренных в нем функций входа в систему и защиты.

Модемом DSL называется устройство, устанавливаемое на одном из концов медного провода и обеспечивающее подключение компьютера (или локальной сети) к Internet с помощью соединения DSL. В отличие от коммутируемого соединения, такому соединению не нужна выделенная телефонная линия (расщепитель линии POTS позволяет разделить линию на несколько каналов). Хотя модемы DSL схожи с обычными аналоговыми модемами, они обеспечивают гораздо большую пропускную способность.

Коммуникационное оборудование

Система использует модемы, адаптер терминала Цифровой сети с комплексными услугами (ISDN), адаптеры кольцевой сети передачи данных с маркерным доступом, адаптеры Ethernet или блоки обслуживания каналов/данных (CSU/DSU) для управления соединениями Протокола двухточечной связи (PPP).

Для создания среды PPP можно использовать четыре типа коммуникационного оборудования:

- Модемы
- CSU/DSU

- Терминальные адаптеры ISDN
- Адаптеры Ethernet (для соединений PPPoE)

Модемы

Для создания соединений PPP применяются как внутренние, так и внешние модемы.

Набор команд, поддерживаемых модемом, описан в инструкции по модему. Эти команды применяются для сброса и инициализации модема, а также для набора номера удаленной системы. Перед применением модема в профайле соединения PPP необходимо его определить, так как для инициализации разных модемов применяются различные командные строки. Строки сброса параметров модема определены только для внутренних модемов.

Система содержит готовые конфигурации для большого числа модемов, однако при необходимости вы можете добавить новую модель с помощью System i Navigator. При создании определения новой линии можно воспользоваться одним из существующих определений. Если у вас нет точной информации о командах модема или нет доступа к его документации, используйте определение модема Generic Hayes. Готовые определения изменять нельзя. Тем не менее, в существующую строку инициализации модема или набора номера можно добавить дополнительные команды.

Для создания соединений PPP может применяться модем электронной поддержки заказчиков (ECS), поставляемый с системой. В более старых системах в качестве модема электронной поддержки заказчиков (ECS) применялся внешний модем IBM 7852-400. Этот модем был заменен на модель MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. В новых системах роль модема ECS выполняют внутренние модемы 2771 или 2772 либо любые другие поддерживаемые модели.

Ссылки, связанные с данной

“Требования к программному и аппаратному обеспечению” на стр. 32
Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров - платформа System i, может быть как инициатором, так и обработчиком соединения.

CSU/DSU

Устройство обслуживания канала (CSU) - это устройство, соединяющее терминал с цифровой линией. Устройство обслуживания данных (DSU) - это устройство для защиты и диагностики телекоммуникационной линии связи. Обычно эти два устройства объединяются в один блок - CSU/DSU.

CSU/DSU можно представить себе как очень мощный и дорогой модем. Для создания соединения T-1 или T-3 необходимо по одному такому устройству для каждой стороны, причем оба устройства должны быть произведены одной фирмой.

Ссылки, связанные с данной

“Требования к программному и аппаратному обеспечению” на стр. 32
Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров - платформа System i, может быть как инициатором, так и обработчиком соединения.

“Цифровая служба и Служба цифровых данных” на стр. 34
С PPP можно использовать цифровые службы и Служба цифровых данных (DDS).

Терминальные адаптеры ISDN

Цифровая сеть с комплексными услугами (ISDN) обеспечивает цифровое соединение для одновременной передачи речевой, цифровой, видео- и прочей информации в произвольном сочетании.

Убедитесь в том, что терминальный адаптер подходит для применения в системе.

Для настройки терминального адаптера выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.

2. Щелкните правой кнопкой мыши на значке **Модемы** и выберите **Новый модем**.
3. В окне диалога **Новый модем** откройте вкладку **Общие** и введите соответствующие значения в **поля**. Убедитесь, что терминальный адаптер ISDN выбран как устройство связи.
4. Выберите вкладку **Параметры ISDN**.
5. Настройте параметры ISDN на вкладке **Параметры ISDN** так, чтобы они соответствовали установленному терминальному адаптеру.

Задачи, связанные с данной

"Пример: Настройка терминального адаптера ISDN" на стр. 58
Этот пример показывает, каким образом настроить терминальный адаптер ISDN.

Ссылки, связанные с данной

"Требования к программному и аппаратному обеспечению" на стр. 32
Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров - платформа System i, может быть как инициатором, так и обработчиком соединения.

"Цифровая сеть с комплексными услугами" на стр. 35
Сеть ISDN обеспечивает цифровую коммутируемую связь. По линиям ISDN можно одновременно передавать как данные, так и голосовую информацию.

Информация о некоторых терминальных адаптерах ISDN:

Существуют терминальные адаптеры нескольких видов.

В качестве внешнего терминального адаптера (модема) Цифровой сети с комплексными услугами (ISDN) рекомендуется выбрать модель **3Com/U.S. Robotics Courier I ISDN V.Everything**. Эта модель поддерживает аналоговые соединения стандарта V.34, стандарт V.90 (X2), стандарт V.92 и многоканальный PPP для ISDN как для входящих, так и для исходящих звонков в системе. Кроме того, этот адаптер автоматически поддерживает Протокол идентификации с квитированием связи по вызову (CHAP) для соединений PPP. Также возможно применение следующих адаптеров терминалов ISDN: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA и ADtran ISU 2x64 Dual Port.

- **Соединения, инициируемые системой.** Courier I самостоятельно идентифицирует удаленный терминальный клиент по протоколу CHAP, а для идентификации соединения с системой применяет Протокол идентификации по паролю (PAP). Таким образом, секретный ответ PAP не передается по соединению ISDN.
- **Соединения, принимаемые системой.** Courier I требует от вызывающей стороны идентификации по протоколу CHAP, если такая идентификация в системе (в соответствии с конфигурацией входящих звонков) необходима. Если система запрашивает идентификацию по протоколу PAP, то терминальный адаптер Courier I выполняет идентификацию по этому протоколу.

Если вы применяете модем Courier I выпуска до 1999 года, то для достижения максимальной производительности соединения ISDN необходимо убедиться, что модем Courier I подключен к системе с помощью кабеля a V.35. С модемом поставляется кабель-переходник от RS-232 к V.35, однако в старых версиях установлен неправильный разъем V.35. По вопросу замены кабеля обратитесь в фирму 3Com/US Robotics.

Примечание: Фирма 3Com/US Robotics заявила о прекращении поставок версии этого терминального адаптера с поддержкой V.35, хотя она еще может поставляться другими фирмами. Версия с поддержкой RS-232 все еще является рекомендуемой, несмотря на ограничение пропускной способности соединений системы значением в 115,2 Кб/с.

Убедитесь в том, что скорость передачи данных по линии V.35 в системе установлена равной 230,4 Кбит/с.

Информация о некоторых терминальных адаптерах ISDN:

Перечисленные здесь терминальные адаптеры более не используются. Их рекомендуется применять только для исходящих удаленных соединений Цифровой сети с комплексными услугами (ISDN) с системой.

3Com Impact IQ ISDN:

Этот терминальный адаптер не рекомендуется применять на платформе System i по следующим причинам:

- Он не поддерживает аналоговые соединения V.34. Тем не менее, этот недостаток можно устранить с помощью внешнего соединения RJ-11.
- Он не поддерживает соединения V.90.
- Он не поддерживает обмен данными с системой на скоростях, превышающих 115 бит/с.
- Он не поддерживает протокол идентификации CHAP. Если задать S84 равным 0, будет выполняться идентификация CHAP.
- Система не в состоянии обнаружить завершение соединения по сигналу DSR от терминального адаптера. Это может привести к нарушению защиты.

Motorola BitSurfr Pro ISDN:

Этот терминальный адаптер не рекомендуется применять на платформе System i по следующим причинам:

- Он не поддерживает аналоговые соединения V.34. Тем не менее, этот недостаток можно устранить с помощью внешнего соединения RJ-11.
- Он не поддерживает соединения V.90.
- Он не поддерживает обмен данными с системой на скоростях, превышающих 115 бит/с.
- Он не поддерживает протокол идентификации CHAP. Несмотря на это, команда @M2=C позволяет выполнять идентификацию CHAP.
- Он не может быть одновременно настроен на ответ как по одноканальным, так и по многоканальным вызовам PPP. Удаленный (вызывающий) терминальный адаптер должен быть настроен на тот же протокол (одноканальный или многоканальный), что и данный адаптер.
- Он не полностью совместим с механизмом аппаратного управления потоком данных, что снижает производительность при работе по многоканальному протоколу PPP. Это приводит к падению производительности при отправке системой данных по многоканальному соединению PPP.

Обработка IP-адресов

Соединения PPP предоставляют несколько вариантов обработки IP-адресов в зависимости от типа профайла соединения.

- DHCP (протокол динамической настройки хостов) может централизованно управлять присвоением IP-адресов в вашей сети. Здесь описаны настройка и управление службами DHCP в вашей сети. См. Протокол динамической настройки хостов (DHCP)
- DNS (сервер имен доменов) предназначен для управления именами хостов и связанными с ними IP-адресами. Здесь описаны настройка и управление службами DNS в вашей сети.См. Система имен доменов
- BOOTP позволяет связать клиентские рабочие станции с системой и присвоить им IP-адреса. Здесь описаны настройка и управление службами BOOTP в вашей сети.См. Протокол начальной загрузки

Ссылки, связанные с данной

“Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

Фильтрация IP-пакетов

Фильтрация IP-пакетов позволяет ограничить доступ отдельного пользователя к различным службам при работе этого пользователя в сети.

Фильтрация пакетов может запрещать или разрешать доступ на основе IP-адресов и/или портов. Каждая стратегия определяет несколько наборов правил фильтрации IP-пакетов с уникальными идентификаторами фильтров PPP. Правила фильтрации пакетов можно создать для одного профайла входящих соединений или для групповой стратегии, которая будет применять их при работе с категорией пользователей. Правила фильтрации пакетов определяются не в PPP, а в окне System i Navigator Правила фильтрации IP-пакетов.

В соединениях L2TP для защиты сетевого потока необходимо применять виртуальную частную сеть (VPN) с фильтрацией IPSEc.

Ссылки, связанные с данной

“Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

Информация, связанная с данной

Фильтрация IP-пакетов и преобразование сетевых адресов

Виртуальная частная сеть (VPN)

Стратегия управления IP-адресами

Перед тем, как вы приступите к настройке профайла соединения PPP, вы должны изучить стратегию управления IP-адресами в вашей сети. Эта стратегия повлияет на множество решений, которые вы примете в процессе настройки, в частности, на выбор стратегии идентификации, соглашений о защите и параметров TCP/IP.

Профайлы исходящих соединений

Обычно локальный и удаленный IP-адреса профайла исходящих соединений задаются с помощью опции *Назначается удаленной системой*.Эта опция позволяет администраторам удаленной системы управлять IP-адресами, применяемыми для создания соединения. Подавляющее число соединений с провайдерами Internet (ISP) устанавливается по этой схеме, хотя многие провайдеры могут предоставить фиксированный IP-адрес за дополнительную плату.

Если локальный или удаленный IP-адреса фиксированы, то вам необходимо убедиться, что удаленная система настроена для работы в такой конфигурации. Обычно фиксируется локальный IP-адрес, а удаленный задается удаленной системой. Система, к которой подключается сервер, может быть настроена аналогичным образом, поэтому при подключении две системы просто обменяются IP-адресами. Этот способ лучше всего подходит для установления временного соединения между двумя офисами.

Существует еще один способ, называемый маскировкой IP-адресов. Например, если система подключена к Internet через провайдера, то сети, подключенные к системе, могут получить доступ к Internet. В этом случае система скроет IP-адреса систем в локальной сети за локальным IP-адресом, выделенным провайдером, а весь поток данных, идущий от систем в локальной сети, будет считаться потоком, идущим от системы. Для того, чтобы весь поток данных от систем в локальной сети отправлялся в систему, необходима небольшая дополнительная настройка маршрутизации в этих системах и системе, в которой необходимо установить флажок **добавить удаленную систему в маршрут по умолчанию**.

Профайлы входящих соединений

В профайлах входящих соединений предусмотрено гораздо больше опций и вариантов выбора IP-адресов, чем в профайлах исходящих соединений. Способ настройки IP-адресов зависит от плана управления IP-адресами в вашей сети, требований к производительности и предоставляемым функциям для данного соединения, а также плана защиты.

Локальные IP-адреса

Для профайла одного входящего соединения можно определить новый уникальный IP-адрес или выделить один из существующих IP-адресов в локальной сети системы для идентификации окончания соединения PPP. Для профайла нескольких входящих соединений необходимо использовать один из существующих локальных IP-адресов. Если таких IP-адресов нет, то для этой цели можно создать виртуальный IP-адрес.

Удаленные IP-адреса

Существует множество вариантов присвоения удаленных IP-адресов клиентам PPP. На странице TCP/IP профайла входящего соединения можно указать следующие опции:

Примечание: Если вы хотите, чтобы удаленная система считалась частью локальной сети, то необходимо настроить маршрутизацию IP-адресов, указать IP-адрес из диапазона адресов систем, подключенных к локальной сети, и убедиться, что пересылка IP включена как в профайле этого соединения, так и в системе.

Таблица 8. Опции присвоения IP-адреса для профайла входящих соединений

Опция	**Описание**
Фиксированный IP-адрес	Вы определяете один IP-адрес, который будет присваиваться удаленным пользователям при подключении. Этот способ подходит только для хостов (при этом маска подсети равна 255.255.255.255), и его можно применять только в профайлах одного входящего соединения.
Пул адресов	Вы определяете начальный IP-адрес и число дополнительных IP-адресов, которые можно выделить. Каждому подключающемуся пользователю будет выделяться уникальный IP-адрес из заданного диапазона. Этот способ подходит только для хостов (при этом маска подсети равна 255.255.255.255), и его можно применять только в профайлах нескольких входящих соединений.
RADIUS	Удаленный IP-адрес и его маска подсети определяются сервером RADIUS. Этот способ можно применять только в том случае, если выполнены следующие условия: • В конфигурации сервера удаленного доступа включена поддержка идентификации и выделения IP-адресов с помощью сервера Radius. • В профайле входящих соединений включена поддержка удаленной идентификации с помощью сервера Radius.
DHCP	Удаленный IP-адрес определяется сервером DHCP либо напрямую, либо косвенно - с помощью агента DHCP. Этот способ применим, только когда в конфигурации сервера удаленного доступа включена поддержка DHCP. Этот способ подходит только для хостов (маска подсети при этом равна 255.255.255.255).
На основе ИД пользователя удаленной системы	Удаленный IP-адрес присваивается при идентификации пользователя удаленной системы в зависимости от указанного ИД. В этом случае системный администратор может выделять разным пользователям, подключающимся к системе, разные IP-адреса и разные маски подсети. Кроме того, это позволяет определять разные дополнительные маршруты для пользователей, настраивая систему для каждого известного удаленного пользователя. Для правильной работы этой функции должна быть включена идентификация.
Определять дополнительные IP-адреса на основе ИД пользователя удаленной системы	Эта опция позволяет определять IP-адреса на основе ИД пользователя удаленной системы. Если удаленный IP-адрес определяется **на основе ИД пользователя удаленной системы**, то эта опция выбирается автоматически и является обязательной. Эту опцию можно также использовать при применении фиксированного IP-адреса и пула адресов. При подключении удаленного пользователя система попытается определить, существует ли IP-адрес, заданный специально для этого пользователя. Если этот адрес существует, то при создании соединения будет использован именно этот IP-адрес, маска подсети и набор дополнительных маршрутов. Если IP-адрес не указан, то по умолчанию будет выбран фиксированный IP-адрес или следующий свободный IP-адрес из пула адресов.

Таблица 8. Опции присвоения IP-адреса для профайла входящих соединений (продолжение)

Опция	Описание
Разрешить удаленной системе определять свой IP-адрес	Эта опция позволяет удаленным пользователям самим определять свои IP-адреса во время начального согласования. Если удаленный пользователь не может определить свой IP-адрес, то система будет применять IP-адрес, заданный с помощью какого-нибудь другого способа выбора удаленного IP-адреса. Изначально эта опция выключена, и к ее применению следует относиться с особой осторожностью.
Маршрутизация IP-адресов	Коммутируемый клиент и система должны правильно настроить маршрутизацию IP-адресов, чтобы клиент мог получить доступ ко всем IP-адресам из локальной сети, которой принадлежит система.

Идентификация систем

Соединения PPP с платформой System i предусматривают несколько вариантов идентификации как удаленных клиентов, подключающихся к системе, так и соединений с провайдером Internet (ISP) или с другим сервером, к которому система.

Система поддерживает несколько способов хранения информация об идентификационных данных - от применения простых контрольных списков содержащих имена и пароли всех пользователей с правами доступа до поддержки серверов RADIUS, хранящих подробную идентификационную информацию обо всех пользователях сети. Система также поддерживает несколько вариантов шифрования ИД и паролей пользователей: от простой смены паролей до поддержки Протокола идентификации с квитированием связи по вызову CHAP-MD5. Вы можете задать параметры идентификации, включая ИД и пароль, идентифицирующие систему в исходящих соединениях, на вкладке **Идентификация** профайла соединения в System i Navigator.

Ссылки, связанные с данной

“Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

“Сценарий: Идентификация коммутируемых соединений с помощью Сервера сетевого доступа (NAS) RADIUS” на стр. 21
Сервер сетевого доступа (NAS), запущенный в системе может направлять запрос на идентификацию от входящих клиентов на отдельный сервер Службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS). После идентификации сервер RADIUS может управлять IP-адресами пользователей.

“Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23
Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Протокол идентификации с квитированием связи по вызову с MD5

Протокол CHAP-MD5 с помощью алгоритма MD-5 вычисляет псевдослучайное значение, которое известно только проверяющей системе и удаленному устройству.

При передаче по протоколу CHAP ИД пользователя и пароль всегда шифруются, поэтому данный протокол безопаснее, чем Протокол идентификации по паролю (PAP). Этот протокол эффективно защищает систему от проникновения методом ″проб и ошибок″, а также с помощью записи сеанса идентификации с последующим повторением. Идентификация может повторяться несколько раз во время работы по протоколу CHAP.

Проверяющая система отправляет запрос удаленному устройству, которое запросило подключение к сети. Удаленное устройство возвращает значение, вычисленное по общему алгоритму (MD-5), который применяется обоими устройствами. Проверяющая система сравнивает ответ с результатом собственных вычислений. Если значения совпадают, то идентификация завершается успешно, в противном случае соединение прерывается.

Ссылки, связанные с данной

"Сценарий: Подключение удаленных клиентов к системе" на стр. 13
Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

"Протокол идентификации по паролю"
Протокол PAP применяет простую процедуру двустороннего обмена для идентификации систем.

Протокол EAP

Протокол EAP позволяет применять при идентификации PPP модули идентификации сторонних производителей.

EAP расширяет протокол PPP с помощью стандартных схем идентификации, таких как передаваемые ключи, система Kerberos, шифрование с открытым ключом и S/Key. EAP позволяет выполнять идентификацию на уровне все возрастающих требований защиты с помощью модулей сторонних производителей. EAP защищает Виртуальную частную сеть (VPN) от взломщиков, применяющих основные типы атак и подбор пароля. EAP также развивает Протокол идентификации по паролю (PAP) и Протокол идентификации с квитированием связи по вызову (CHAP).

При применении протокола EAP идентификационная информация передается как часть основной информации. Это позволяет системам согласовывать необходимые параметры защиты до приема или передачи основной информации.

Система не поддерживает EAP напрямую. Однако при применении службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS) вы сможете применять описанные выше схемы идентификации.

Протокол идентификации по паролю

Протокол PAP применяет простую процедуру двустороннего обмена для идентификации систем.

Обмен выполняется при установлении соединения. После установления связи удаленное устройство передает ИД пользователя и пароль проверяющей системе. Если передана правильная пара значений, то сеанс продолжается, в противном случае связь прерывается.

При идентификации с протоколом PAP ИД пользователя и пароль пересылаются по сети в виде текста. Протокол PAP не предусматривает шифрования ИД пользователя и пароля, что делает возможным их перехват. По этой причине рекомендуется всегда использовать протокол идентификации с квитированием связи по вызову (CHAP).

Ссылки, связанные с данной

"Протокол идентификации с квитированием связи по вызову с MD5" на стр. 45
Протокол CHAP-MD5 с помощью алгоритма MD-5 вычисляет псевдослучайное значение, которое известно только проверяющей системе и удаленному устройству.

Обзор службы дистанционной аутентификации пользователей по коммутируемым линиям

Служба RADIUS - это протокол Internet, который позволяет применять центральный сервер для идентификации, ведения учетных записей и обслуживания удаленных пользователей в распределенной модемной сети.

В архитектуре RADIUS роль клиента выполняет сервер доступа к сети (NAS), подключающийся к серверу RADIUS. Система, работающий в качестве NAS, отправляет информацию о пользователе и соединении выделенному серверу RADIUS с помощью стандартного протокола RADIUS, определенного в RFC 2865.

Серверы RADIUS идентифицируют пользователя и отправляют NAS всю необходимую информацию о конфигурации, позволяющую NAS (системе) предоставлять удаленным пользователям необходимые услуги.

Если сервер RADIUS недоступен, то система может переслать запрос на идентификацию альтернативному серверу. Это, в свою очередь, позволяет глобальным организациям предоставлять пользователям доступ с помощью модема и выполнять идентификацию ИД пользователя и пароля независимо от точки доступа.

При получении сервером RADIUS запроса на идентификацию он проверяет запрос и расшифровывает пакет данных для извлечения имени пользователя и пароля. Эта информация передается соответствующей системе защиты. Такой системой могут быть файлы паролей UNIX, система Kerberos, коммерческая система защиты и даже пользовательская система защиты. Сервер RADIUS отправляет в систему все данные, для работы с которыми у пользователя есть права доступа, такие как IP-адрес. Запросы учета RADIUS обрабатываются аналогично. Учетные запросы RADIUS обрабатываются таким же образом. Информация об учетной записи удаленного пользователя может быть отправлена серверу учетных записей RADIUS. Стандартный протокол ведения учетных записей RADIUS описан в RFC 2866. Сервер учетных записей RADIUS обрабатывает запросы в соответствии с протоколом учетных записей RADIUS.

Ссылки, связанные с данной

“Сценарий: Идентификация коммутируемых соединений с помощью Сервера сетевого доступа (NAS) RADIUS” на стр. 21
Сервер сетевого доступа (NAS), запущенный в системе может направлять запрос на идентификацию от входящих клиентов на отдельный сервер Службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS). После идентификации сервер RADIUS может управлять IP-адресами пользователей.

Контрольный список

В контрольном списке хранятся ИД и пароли удаленных пользователей.

Вы можете применять существующий контрольный список или создать собственный на странице идентификации профайла входящих соединений. В записях контрольного списка необходимо также указывать протокол идентификации, связанный с ИД пользователя и паролем. Этим протоколом может быть **шифрованный - CHAP-MD5/EAP** или **нешифрованный - PAP**.

Инструкции по выполнению этой задачи можно найти в электронной справке.

Ссылки, связанные с данной

“Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23
Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Полоса пропускания многоканального соединения

Иногда для выполнения определенных задач возникает потребность во временной дополнительной полосе пропускания.

Приобретение дополнительного специализированного оборудования может быть неоправданным. Многоканальный протокол PPP (MP) объединяет несколько физических соединений PPP в один виртуальный канал. Общая полоса пропускания такого канала будет больше суммы полос пропускания отдельных каналов в силу более рационального использования модемов и телефонных линий. В комплект MP может входить до шести линий. Для создания многоканального соединения протокол MP должен поддерживаться обеими сторонами соединения PPP. Многоканальный протокол описан в документе RFC-1990.

Полоса пропускания по запросу

Возможность динамически изменять число физических линий связи позволяет настроить в системе режим, при котором расширенная полоса пропускания создается только в том случае, когда это действительно необходимо. Этот способ обычно называют Полоса пропускания по запросу. Он позволяет платить за дополнительное соединение только в том случае, если оно реально используется. Для наиболее рационального использования преимуществ такого подхода рекомендуется включить монитор общей полосы пропускания комплекта MP хотя бы на одном узле. При этом, если полоса пропускания используется сильнее или слабее, чем это предусмотрено конфигурацией, в комплект MP можно добавить или удалить дополнительные линии связи. Протокол BAP позволяет системам проводить согласование перед добавлением или удалением линий связи в комплект MP. В документе RFC-2125 описан как протокол BAP, так и протокол BACP.

Информация, связанная с данной

Редактор RFC

Настройка PPP

Перед созданием соединения PPP необходимо настроить среду PPP.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Создание профайла соединения

Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Профайл соединения содержит информацию о следующих параметрах соединения:

- Тип профайла и линии связи
- Параметры многоканального соединения
- Номера удаленных телефонов и опции набора номера
- Сведения об идентификации
- Параметры TCP/IP: IP-адреса и маршрутизация
- Управление работой и настройка соединений
- Сервер имен доменов

Раздел **Службы удаленного доступа** каталога Сеть содержит следующие объекты:

- Профайлы исходящих соединений
- Профайлы входящих соединений
- **Модемы**

Для создания профайла соединения выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Выберите одну из следующих опций:
   - Для того чтобы сделать систему инициализатором, щелкните правой кнопкой мыши на пункте **Профайлы исходящих соединений**.
   - Щелкните правой кнопкой мыши на пункте **Профайлы входящих соединений** и выберите систему в качестве принимающего входящие соединения от удаленных систем и пользователей.
3. Выберите **Новый профайл**.
4. На странице Настройка нового профайла соединения PPP выберите тип протокола.

5. Задайте режим выбора.
6. Выберите конфигурацию канала.
7. Нажмите **OK**.

   Появится страница Свойства нового профайла PPP. На ней можно указать остальные параметры сети. Более подробная информация приведена в электронной справке.

   Задачи, связанные с данной

   “Связывание модема с описанием линии” на стр. 58
   В данном разделе приведена информация о связывании модема с описанием линии.

   Ссылки, связанные с данной

   “Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
   Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

   “Сценарий: Подключение удаленных клиентов к системе” на стр. 13
   Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

   “Сценарий: Подключение локальной сети к Internet с помощью модема” на стр. 15
   Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Систему можно подключить к ISP с помощью модема. Клиенты PC, подключенные к сети, будут использовать операционную систему i5/OS в качестве шлюза при доступе к Internet.

   “Сценарий: Подключение сети филиала компании к основной сети с помощью модема” на стр. 18
   Модем позволяет обмениваться данными между двумя расположениями (такими, например, как центральный офис и филиал). Две сети можно объединить с помощью соединения PPP, подключив одну сеть к системе в центральном офисе, а другую - к другой в офисе филиала компании.

   “Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23
   Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Тип протокола: PPP или SLIP

PPP постепенно вытесняет SLIP с рынка двухточечных соединениях.

PPP позволяет взаимодействовать сетевому программному обеспечению от различных производителей. Он также позволяет нескольким протоколам сетевых соединений использовать одну линию связи.

Протокол SLIP не стал стандартом Internet из-за следующих недостатков:

- У этого протокола нет стандартных способов для IP-адресации между двумя хостами. Это делает применение ненумерованной сети невозможным.
- SLIP не поддерживает обнаружение и сжатие ошибок. Эти функции поддерживаются протоколом PPP.
- SLIP также не поддерживает идентификацию системы, в то время как в PPP реализована двусторонняя идентификация.

Протокол SLIP по-прежнему применяется и по-прежнему поддерживается операционной системой i5/OS. Тем не менее, IBM рекомендует по возможности применять протокол PPP. SLIP не поддерживает многоканальные соединения. По сравнению со SLIP, в протоколе PPP лучше реализована идентификация. Применение протокола PPP более предпочтительно из-за поддержки этим протоколом сжатия данных.

Примечание: Протоколы SLIP с типами линий ASYNC не поддерживаются в этом выпуске. Если в системе есть профайлы таких соединений, то их рекомендуется преобразовать в профайлы SLIP или профайлы PPP с типом линии PPP.

Выбор режима

Выбор режима в профайле соединения PPP состоит из выбора типа соединения и выбора режима работы. Выбор режима задает способ применения нового соединения PPP.

Для выбора режима выполните следующие действия:

1. Выберите один из следующих типов соединения:
   - Коммутируемая линия
   - Выделенная линия
   - Протокол туннеля второго уровня (L2TP) (виртуальная линия)
   - Двухточечный протокол по линии Ethernet (PPPoE)
2. Выберите соответствующий режим работы нового соединения PPP.
3. Запишите выбранный тип линии и режим работы. Эта информация понадобится при настройке соединений PPP.

Коммутируемая линия:

При использовании внутреннего или внешнего модема или адаптера терминала ISDN для соединения по телефонной линии выберите Соединение по коммутируемой линии.

Коммутируемая линия может работать в следующих режимах:

Ответ

Выберите этот режим работы для ответа системы на вызовы удаленной системы.

Набор номера

Выберите этот режим работы для набора системой номера удаленной системы.

Набор номера по запросу (только набор номера)

Выберите этот режим работы для автоматического набора системой номера удаленной системы при получении от нее пакетов TCP/IP. Соединение закрывается, когда передача данных завершена и на протяжении определенного промежутка времени данные TCP/IP не передаются.

Набор номера по запросу (с ответом определенной системе)

Выберите этот режим работы для ответа системы на вызовы выделенной удаленной системе. Этот режим работы также позволяет системе вызывать удаленную систему при получении от нее пакетов TCP/IP. Если на обеих сторонах соединения работают операционные системыi5/OS в данном режиме, то данные TCP/IP передаются от одной системы к другой по мере необходимости, не требуя создания постоянного физического соединения. Для работы в этом режиме необходим выделенный ресурс. Для правильной работы этого режима удаленная система также должна быть правильно настроена на набор номера.

Набор номера по запросу (с поддержкой нескольких удаленных систем)

Выберите этот режим работы для ответа удаленной системе или набора ее номера. Для обработки входящих звонков необходимо указать существующий профайл ответа соединения PPP, в котором задан данный режим работы. Это позволяет использовать один профайл ответа для обработки всех входящих звонков от одной или нескольких удаленных систем, и отдельный профайл набора номера по запросу для каждого исходящего звонка. Этот режим работы не требует постоянного выделения ресурса для обработки звонков от удаленных систем.

Выделенная линия:

Выберите тип соединения - выделенная линия, если система соединена с удаленной системой по выделенному физическому каналу. При наличии выделенной линии для соединения двух систем не требуется модем или терминальный адаптер ISDN.

Выделенными называются линии, постоянно соединяющие две системы или специально зарезервированные для связи между ними. Выделенные линии всегда открыты. При соединении по выделенной линии одна сторона настраивается как вызывающая, а другая - как отвечающая.

Выделенная линия может работать в следующих режимах:

Ответ

Выберите этот режим работы для предоставления удаленной системе доступа к системе по выделенной линии. Этот режим работы предназначен для профайла ответа выделенной линии.

Вызов

Выберите этот режим работы для доступа системы к удаленной системе по выделенной линии. Этот режим работы предназначен для профайла набора номера выделенной линии.

L2TP (виртуальная линия):

Выберите этот тип связи для соединения двух систем по Туннельному протоколу второго уровня (L2TP).

Виртуальное соединение PPP между локальной и удаленной системой устанавливается сразу после организации туннеля L2TP. Туннели L2TP в сочетании с протоколом защиты IP (IP-SEC) позволяют организовать передачу, маршрутизацию и прием защищенных данных через Internet.

Линия L2TP (виртуальная линия) может работать в следующих режимах:

Ответ

Выберите этот режим работы для предоставления удаленной системе доступа к системе по туннелю L2TP.

Вызов

Выберите этот режим работы для предоставления системе доступа к удаленной системе по туннелю L2TP.

Удаленный набор номера

Выберите этот режим работы для подключения системы к провайдеру по туннелю L2TP и передачи провайдеру указания на набор номера удаленного клиента PPP.

Транзитный вызов

Выберите этот режим работы для создания системой транзитного соединения.

Примечание: У профайла ответа L2TP должна быть выбрана опция **Разрешить транзитное соединение**, и должен существовать контрольный список PPP, связывающий имя пользователя PPP с профайлом вызова транзитного соединения.

Линия PPPoE:

Соединения PPPoE применяют виртуальные линии для отправки данных PPP через выделенные адаптеры Ethernet на предоставленный провайдером Internet модем DSL. Модем также подключен к локальной сети Ethernet.

Это обеспечивает высокоскоростной доступ к Internet для пользователей локальной сети с помощью соединения PPP операционной системыi5/OS. После установления соединения между системой и провайдером Internet (ISP) пользователи локальной сети (LAN) получают доступ к ISP по соединению PPPoE.

Соединения PPPoE используются только профайлами исходящих соединений. Они подразумевают режим работы Вызов и применяют только отдельную линию.

Конфигурация линии связи

Конфигурация линии связи задает тип линии, применяемый для создания соединения PPP.

Тип линии зависит от выбранного типа соединения.

Ссылки, связанные с данной

“Сценарий: Подключение системы к концентратору PPPoE” на стр. 10
Многие ISP предлагают высокоскоростной доступ к Internet по DSL, используя двухточечный PPP для Ethernet (PPPoE). Это дает высокоскоростной доступ с сохранением преимуществ соединений по протоколу двухточечной связи (PPP).

“Сценарий: Подключение удаленных клиентов к системе” на стр. 13
Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

“Сценарий: Подключение локальной сети к Internet с помощью модема” на стр. 15
Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Систему можно подключить к ISP с помощью модема. Клиенты PC, подключенные к сети, будут использовать операционную систему i5/OS в качестве шлюза при доступе к Internet.

“Сценарий: Подключение сети филиала компании к основной сети с помощью модема” на стр. 18
Модем позволяет обмениваться данными между двумя расположениями (такими, например, как центральный офис и филиал). Две сети можно объединить с помощью соединения PPP, подключив одну сеть к системе в центральном офисе, а другую - к другой в офисе филиала компании.

Отдельная линия:

Выберите эту службу, если соединения PPP будут устанавливаться через аналоговый модем. Это значение также применяется для выделенных линий, подключаемых к системе напрямую (без модема). Профайл соединения PPP всегда применяет один и тот же ресурс порта связи i5/OS.

Аналоговая отдельная линия может быть настроена как `общая` для профайлов исходящего и входящего соединений (профайлов вызова и ответа). Динамическое разделение ресурсов - это новая функция, повышающая эффективность использования ресурсов. До версии V5R2 ресурсы модема использовались только в случае запуска соответствующего профайла соединения. Это позволяло выделять пользователю только один ресурс в сеансе, даже если ресурс находился в состоянии пассивного ожидания. Теперь новые правила совместного использования вступают в силу при обращении к определенному ресурсу. Возможны два варианта. Первый - когда профайл вызова был запущен до профайла ответа. Второй - когда, наоборот, профайл ответа был запущен до профайла вызова. Предполагается, что совместное использование ресурсов включено. В первом случае запущенный профайл вызова установит соединение. Профайл ответа, запущенный вторым, будет ждать освобождения линии. После завершения исходящего соединения профайл ответа запросит линию и установит соединение. Во втором случае запущенный профайл ответа будет ждать запросов входящих соединений. На то время, пока такие запросы отсутствуют, профайл вызова, запущенный вторым, ″одолжит″ линию у профайла ответа. После этого будет установлено исходящее соединение. После завершения этого соединения профайл вызова вернет линию профайлу ответа, который снова будет готов принять входящее соединение. Для включения режима совместного использования перейдите к вкладке **Модем**, соответствующей описанию коммутируемой линии, и выберите пункт **Включить динамическое совместное использование ресурсов**.

Отдельная линия также применяется при создании соединений L2TP (виртуальных линий)и PPPoE (виртуальных линий). При создании соединений L2TP (виртуальных линий) с применением одной линии ресурсы порта связи не требуются. Соединение L2TP с применением одной линии называется *виртуальным* потому, что для организации туннеля не требуется физический ресурс PPP.Отдельная линия, применяемая для соединений PPPoE, также является виртуальной и предоставляет механизмы для работы с физической линией Ethernet как с линией PPP, поддерживающей удаленные соединения. Виртуальная линия PPPoE связана с физической линией Ethernet и используется для поддержки передачи данных PPP по соединению LAN Ethernet с модемом DSL.

Пул линий:

Выберите этот тип для создания соединения PPP с применением линии из пула линий. При создании соединения PPP система выбирает из пула незанятую линию. Для профайлов набора номера по запросу линия не выбирается до тех пор, пока система не обнаружит пакеты TCP/IP, которые необходимо отправить удаленной системе.

В профайле соединения пул линий можно указать вместо конкретного описания линии. Пул линий позволяет указать одно или несколько описаний линии.

Пул линий позволяет применять профайл соединения для обработки нескольких входящих звонков по аналоговой линии или одного исходящего звонка. После завершения соединения PPP линия возвращается в пул линий.

При применении пула линий для одновременной обработки нескольких входящих звонков необходимо указать максимальное число входящих соединений. Это значение можно задать на вкладке **Соединения** окна диалога **Свойства нового профайла PPP** при настройке профайла соединения. Для применения пулов линий с одиночными соединениями с повышенной пропускной способностью необходимо использовать многоканальную линию.

Преимущества пулов линий:

- Линия не выделяется профайлу соединения PPP до его запуска.

  Если в профайле PPP указана конкретная линия, то соединение не устанавливается, когда линия недоступна, если только не включено динамическое совместное использование ресурсов. Для установления соединений, использующих пул, достаточно наличия хотя бы одной свободной линии в пуле.

  Если ресурсы были настроены в качестве общих (включено динамическое совместное использование ресурсов), то повышенная готовность ресурсов обеспечивается прежде всего для исходящих соединений.
- С пулами линий могут применяться профайлы с набором номера по запросу, обеспечивающие более эффективное распределение ресурсов.

  Система занимает линию из пула только на время установления соединения для передачи данных. В другое время эту линию можно использовать для создания других соединений.
- Для создания большего числа соединений PPP необходимо меньшее число ресурсов.

  Например, если необходима возможность установить четыре различных типа соединений, однако в любой момент времени требуются только две линии, то для создания такой среды можно воспользоваться пулом линий. Создайте четыре профайла с набором номера по запросу, каждый из которых должен ссылаться на пул из двух линий. Каждая линия будет доступна всем профайлам, поэтому в любой момент времени можно будет установить два соединения. Применение пула линий позволяет в подобной ситуации использовать две линии вместо четырех.

  Если среда является средой и клиента PPP, и сервера PPP, то линии могут быть общими (т.е. возможно динамическое совместное использование ресурсов) независимо от того, являются ли они 'отдельными линиями' или помещены в 'пул линий'. Профайл, запущенный первым, не будет фиксировать ресурс, пока соединение не станет активным. Например, если запущен сервер PPP, то на время, пока он ожидает запросов входящих соединений, он 'одолжит' линию запущенному клиенту PPP.

Настройка пулов линий

Пулы линий определяются в профайле соединения. Для настройки основных параметров пула линий выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Создайте профайл соединения для исходящих или входящих соединений. Выберите одну из следующих опций:
   - Для того чтобы сделать систему инициализатором модемных соединений с удаленной системой, щелкните правой кнопкой мыши на пункте **Профайлы исходящих соединений**.

- Щелкните правой кнопкой мыши на пункте **Профайлы входящих соединений** и выберите систему в качестве принимающего входящие соединения от удаленных систем и пользователей.

3. Выберите **Создать профайл**.
4. Для профайла исходящего соединения (набор номера) установите следующие значения: PPP, Коммутируемая линия и Режим работы (обычно набор номера). В качестве конфигурации линии выберите **Пул линий**.Нажмите **OK**. В окне System i Navigator появится окно свойств данного профайла соединения.

   Примечание: Пул линий можно также выбрать при создании профайла входящих соединений. Значение Пул линий может быть как показано, так и не показано, в зависимости от выбранного типа протокола, типа соединения и режима работы.
5. На вкладке Общие укажите имя профайла и задайте описание.
6. На вкладке Соединение введите имя пула линий и нажмите кнопку **Создать**. После этого на экране появится окно диалога **Свойства нового пула линий**, в котором будут перечислены все доступные линии и модемы системы.
7. Выберите линии, которые необходимо использовать, и добавьте их в пул. Можно также определить новую линию с помощью кнопки **Создать линию**.
8. Для сохранения пула линий нажмите **OK** и перейдите к окну Свойства нового двухточечного профайла.
9. Задайте на остальных страницах необходимые данные (например, параметры TCP/IP и данные идентификации).
10. Для профайла соединения будут последовательно просматриваться все доступные линии в пуле, до тех пор, пока не будет найден свободный ресурс. Дополнительная информация приведена в справочной системе System i Navigator.

Ссылки, связанные с данной

“Сценарий: Подключение удаленных клиентов к системе” на стр. 13
Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к системе с помощью соединения по Протоколу двухточечной связи (PPP).

“Сценарий: Подключение локальной сети к Internet с помощью модема” на стр. 15
Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Систему можно подключить к ISP с помощью модема. Клиенты PC, подключенные к сети, будут использовать операционную систему i5/OS в качестве шлюза при доступе к Internet.

“Сценарий: Подключение сети филиала компании к основной сети с помощью модема” на стр. 18
Модем позволяет обмениваться данными между двумя расположениями (такими, например, как центральный офис и филиал). Две сети можно объединить с помощью соединения PPP, подключив одну сеть к системе в центральном офисе, а другую - к другой в офисе филиала компании.

Профайл с поддержкой нескольких соединений:

Профайл PPP с поддержкой нескольких соединений позволяет использовать один профайл для обслуживания нескольких вызовов по аналоговым или цифровым линиям, а также туннелям L2TP.

Эта возможность полезна в том случае, если к системе должно подключаться несколько пользователей, но вы не хотите создавать отдельный профайл для каждой линии связи PPP. Она наиболее часто применяется в случае встроенного 4-портового модема 2805, когда четыре линии обслуживаются одним адаптером.

Число линий из пула, используемых профайлами с поддержкой нескольких соединений, ограничено параметром Максимальное число соединений. Фактически для каждой линии пула запускается собственная нить профайла, и, благодаря этому, профайл ожидает поступления вызовов по всем линиям одновременно.

Локальный IP-адрес для профайлов с поддержкой нескольких соединений

В профайлах с поддержкой нескольких соединений могут применяться локальные IP-адреса, которые определены в системе. Для выбора IP-адреса при настройке применяется выпадающий список Локальные IP-адреса. Выбор IP-адреса в качестве локального IP-адреса для профайла PPP позволяет клиентам, подключающимся по соответствующему соединению, работать с ресурсами локальной сети. При этом адреса, входящие в пул удаленных IP-адресов, должны находиться в одной сети с локальным IP-адресом.

Если локальный IP-адрес отсутствует или вы не хотите, чтобы удаленные пользователи получали доступ к локальной сети, системе необходимо присвоить виртуальный IP-адрес. Виртуальный IP-адрес также называется адресом виртуального интерфейса. Такой адрес может применяться в качестве локального IP-адреса в профайлах соединений PPP. В связи с тем, что виртуальный IP-адрес не связан с физической сетью, он не позволяет автоматически перенаправлять данные в сетях, к которым подключена локальная система.

Для создания виртуального IP-адреса выполните следующие действия:

1. В System i Navigatorвыберите свою систему и откройте раздел **Сеть → Настройка TCP/IP → IPV4 → Интерфейсы**.
2. Щелкните правой кнопкой мыши на пункте **Интерфейсы** и выберите пункт **Создать интерфейс → Виртуальный IP**.
3. Следуйте инструкциям Мастера создания интерфейсов. Виртуальный IP-адрес может применяться в профайле соединения сразу после создания. Для выбора этого IP-адреса также применяется выпадающий список **Локальный IP-адрес** на странице параметры TCP/IP.

   Примечание: Виртуальный IP-адрес должен быть активен до запуска профайла; в противном случае, профайл не будет запущен из-за ошибки. Для активации IP-адреса после создания интерфейса во время работы с мастером создания интерфейсов необходимо выбрать опцию запуска.

Пулы удаленных IP-адресов для профайлов с поддержкой нескольких соединений

Можно использовать удаленные пулы IP-адресов с профайлами нескольких соединений. Обычный профайл PPP, поддерживающий одно соединение, жестко связан с одним удаленным IP-адресом, который присваивается вызывающей системе при установлении соединения. Поскольку к профайлу, поддерживающему несколько соединений, могут одновременно подключиться несколько удаленных систем, то для назначения IP-адресов вызывающим системам применяется начальный удаленный IP-адрес и диапазон адресов.

Ограничения на использование пула линий

При использовании пулов линий в профайлах с поддержкой нескольких соединений существуют следующие ограничения:

- В каждый момент времени линия может принадлежать только одному пулу. Если вы удалите линию из пула, ее можно будет добавить в другой пул.
- Число линий из пула, используемых профайлами с поддержкой нескольких соединений, ограничено параметром Максимальное число соединений. Если свободные линии отсутствуют, то установить новые соединения нельзя. Кроме того, если в пуле нет линий, то в случае запуска нового профайла его работа будет автоматически завершена.
- После запуска профайла с одним соединением, с которым связан пул линий, занятой оказывается только одна линия из пула. Если для того же пула линий будет запущен профайл с поддержкой нескольких соединений, то остальные линии будут доступны для использования.

Задачи, связанные с данной

“Этап 1: Настройка профайла терминатора L2TP для любого интерфейса раздела, в котором расположены модемы” на стр. 28
Для создания профайла вызываемой стороны для любого интерфейса выполните следующие действия:

Пулы удаленных IP-адресов:

Пулы удаленных IP-адресов могут применяться любым профайлом PPP, используемым для обработки нескольких входящих соединений.

К числу таких соединений относятся соединения по L2TP и соединения по линиям из пула с максимально допустимым числом соединений, большим 1. Пулы удаленных адресов позволяют присваивать уникальный IP-адрес каждой подключающейся системе.

Первая удаленная система, с которой будет установлено соединение, получит IP-адрес, указанный в поле Начальный IP-адрес. Если этот IP-адрес будет занят, то удаленной системе будет выделен первый доступный IP-адрес из диапазона. Предположим, что в поле Начальный IP-адрес указано значение 10.1.1.1, а в поле Число IP-адресов - значение 5. В этом случае пул будет состоять из следующих IP-адресов: 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 и 10.1.1.5. Для пула удаленных IP-адресов всегда применяется маска подсети 255.255.255.255.

На применение пулов удаленных IP-адресов установлены следующие ограничения:

- Один и тот же пул адресов может применяться несколькими профайлами. Однако, если на данный момент все IP-адреса из пула уже заняты, то все последующие запросы на соединение будут отклоняться до тех пор, пока не освободится какой-нибудь IP-адрес.
- Для того чтобы присвоить фиксированные IP-адреса набору конкретных систем и позволить остальным системам динамически получать IP-адреса из пула, выполните следующие действия:
  1. Включите опцию Идентификация удаленных систем на странице **Идентификация** для определения имени пользователя удаленной системы.
  2. Определите пул удаленных IP-адресов для всех систем, не требующих фиксированного адреса.
  3. Задайте удаленные IP-адреса конкретных пользователей с помощью переключателя **Определять удаленные IP-адреса на основе ИД пользователя удаленной системы** и кнопки **IP-адреса для ИД пользователя**.

  При подключении удаленного пользователя система сначала проверяет, назначен ли ему фиксированный IP-адрес. Если фиксированный IP-адрес назначен, то он автоматически присваивается удаленной системе. В противном случае, для нее выбирается IP-адрес из пула IP-адресов.

Настройка модема для работы с PPP

Модем обеспечивает возможность аналогового соединения (по выделенной или коммутируемой линии). Для аналоговых соединений по Протоколу двухточечной связи (PPP) может применяться внешний модем, внутренний модем или терминальный адаптер Цифровой сети с комплексными услугами (ISDN).

Ссылки, связанные с данной

“Устранение неполадок PPP” на стр. 66
При обнаружении неполадок PPP можно воспользоваться справочной таблицей для сбора информации об ошибках. Эта справочная таблица поможет вам при обнаружении и устранении неполадок соединений PPP.

Настройка нового модема

Можно настроить новый модем с помощью существующего описания модема или создать описание модема на основании предыдущего описания модема.

Для настройки нового модема выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на значке **Модемы** и выберите **Новый модем**.

3. На вкладке **Общие** укажите требуемые значения в полях.
4. Необязательно: Откройте вкладку **Дополнительные параметры** и добавьте необходимые команды инициализации для своего модема.
5. Нажмите **OK** для сохранения записей и закройте окно Свойства нового модема.

Использование существующего описания модема

Для того чтобы найти существующее описание модема, выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Выберите **Модемы**.
3. В списке описаний модемов найдите название, модель и версию своего модема.

   Примечание: Если ваш модем есть в списке, никаких дополнительных действий выполнять не требуется.
4. Щелкните правой кнопкой мыши на описании модема, наиболее близкого по своим параметрам к вашему, и выберите **Свойства** для просмотра командных строк.
5. Найдите командные строки своего модема в его документации.

   Если они соответствуют показанным на экране, вы можете использовать существующее описание модема. В противном случае вам понадобится создать описание модема и добавить его в список.

Создание нового описания модема на основе предыдущего

Для создания описания модема выполните следующие действия:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Выберите **Модемы**.
3. В списке модемов щелкните правой кнопкой мыши на строке **Стандартный hayes-совместимый** и выберите **Создать модем на основе выбранного**.
4. В окне диалога **Создать модем** введите командные строки, соответствующие модему.

   Ссылки, связанные с данной

   “Устранение неполадок PPP” на стр. 66
   При обнаружении неполадок PPP можно воспользоваться справочной таблицей для сбора информации об ошибках. Эта справочная таблица поможет вам при обнаружении и устранении неполадок соединений PPP.

Задание командных строк модема

Командные строки, соответствующие вашему модему, должны быть приведены в его документации. При создании модема укажите параметры, рекомендованные его производителем.

Таблица 9. Модемы, определенные в системе и текст команд

Функция настройки модема	**Команда для большинства модемов**
Сброс модема с установкой параметров по умолчанию	AT&F или AT&Z
Инициализация модема:	
Вывод текстовых сообщений	Q0 и V1
Обычные режимы CD и DTR	&C1 и &D2
Отключение эхоповтора	E0
DSR после возврата каретки	&S1
Включить аппаратное управление потоком (RTS/CTS)	
Включить исправление ошибок и (необязательно) сжатие данных (V.42/V.42 bis)	

Таблица 9. Модемы, определенные в системе и текст команд (продолжение)

Функция настройки модема	**Команда для большинства модемов**
Убедиться, что быстродействие линии DTE-DCE равно 115,2 Кбит/с (или максимальному значению модема)	
(Необязательно) Включить таймер простоя, если модем поддерживает эту функцию	
Режим ответа модема:	
Ответ после *n* звонков	S0=*n*, где *n* = 1 или 2
Отсоединение при отсутствии несущей частоты (соединения) через *m* секунд	S7=*m*
Способ набора номера	ATDT - тоновый набор, ATDP - для импульсный

Пример: Настройка терминального адаптера ISDN

Этот пример показывает, каким образом настроить терминальный адаптер ISDN.

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на значке **Модемы** и выберите **Новый модем**.
3. На вкладке **Общие** укажите требуемые значения в **полях**.
4. Необязательно: Откройте вкладку **Параметры ISDN** и добавьте необходимые команды инициализации для своего модема.

   Команды и параметры из этого списка передаются терминальному адаптеру ISDN только при соблюдении следующих условий:

   - При изменении или добавлении какой-либо команды или ее параметров
   - При восстановлении после ошибки, выполняемом системой

   Эти команды должны выполнять только следующие задачи:

   - Задавать тип и версию коммутатора ISDN телефонной компании.
   - Задавать номер линии (LDN) и коды доступа (SPID), предоставленные телефонной компанией.
   - Задавать Идентификаторы терминала (TEI), предоставленные телефонной компанией.
   - Задавать протокол B-канала (соединение асинхронного и синхронного PPP).
   - Задавать другие строки настройки переменной длины, содержащие переносы строки.
   - Сохранять и восстанавливать конфигурацию модема после его сброса или выключения системы.
   - Команда проверки состояния интерфейса *U* (ATD*x*) which позволяет системе определить, установлено ли соединение с центральным коммутатором ISDN. Вместо *x* может стоять любая цифра, а также символ # или *.
5. Нажмите кнопку **Добавить** для добавления дополнительных команд модема.Команды можно добавлять со связанным параметром или без него, а также с кратким описанием. Если вы не укажете параметры команды, это можно будет сделать при добавлении модема в описание линии.
6. Нажмите **OK** для сохранения записей и закройте окно Свойства нового модема.

Ссылки, связанные с данной

“Терминальные адаптеры ISDN” на стр. 40
Цифровая сеть с комплексными услугами (ISDN) обеспечивает цифровое соединение для одновременной передачи речевой, цифровой, видео- и прочей информации в произвольном сочетании.

Связывание модема с описанием линии

В данном разделе приведена информация о связывании модема с описанием линии.

1. В System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа → Профайлы исходящих соединений или Профайлы входящих соединений**.
2. Выберите одну из следующих опций:

- Для работы с существующим профайлом соединения щелкните правой кнопкой мыши на профайле и выберите **Свойства**.
- Для работы с новым профайлом соединения создайте новый профайл.

3. В окне свойств нового профайла PPP выберите вкладку **Соединение** и нажмите **Создать**.
   - Введите имя конфигурации линии связи.
   - Для перехода к окну свойств новой линии связи нажмите **Создать**.
4. В окне свойств новой линии связи выберите вкладку **Модем** и выберите модем из списка. Выбранный модем будет связан с описанием линии. Для внутренних модемов соответствующее определение модема к этому моменту уже должно быть выбрано. Дополнительная информация приведена в электронной справке.

Для профайлов исходящих соединений можно настроить ″временное использование″ линии PPP и модема, выделенного профайлу входящего соединения, ожидающего входящего вызова. Исходящее соединение вернет линию PPP и модем профайлу входящего соединения после завершения соединения. Для включения этой функции выберите опцию **Включить динамическое совместное использование ресурсов** на вкладке **Модем** окна Настройка линии PPP. Для настройки линий PPP служит вкладка **Соединения** меню Профайлы входящих и исходящих соединений.

Задачи, связанные с данной

“Создание профайла соединения” на стр. 48
Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на в системе.

Настройка удаленного PC

Для подключения к платформе System i с персонального компьютера, работающего под управлением 32-разрядной операционной системы Windows,, необходимо убедиться в том, что модем установлен и правильно настроен, а на персональном компьютере установлены протокол TCP/IP и Удаленный доступ к сети.

Информация о настройке удаленного доступа к сети в системах PC приведена в документации по Microsoft Windows. Убедитесь в том, что была задана следующая информация:

- Типом модемного соединения должен быть **PPP**.
- При применении зашифрованных паролей убедитесь в том, что применяется протокол CHAP-MD5 (MS-CHAP НЕ поддерживается операционной системой i5/OS). Некоторые версии Windows не поддерживают MD-5 CHAP по умолчанию, но эту поддержку можно настроить с помощью дополнительных справочных материалов Microsoft.
- При применении незашифрованных (или незащищенных) паролей будет автоматически использоваться протокол PAP. Это единственный незащищенный протокол, поддерживаемый системой.
- Обычно адресация IP задается удаленной системой или операционной системой i5/OS. Для применения альтернативных способов адресации IP (таких как задание своих IP-адресов) необходимо убедиться в том, что система принимает адреса, задаваемые пользовательскими способами.
- Если в среде есть сервер DNS, укажите его IP-адрес.

Настройка доступа к Internet с помощью AT&T Global Network

Если требуется установить соединение с AT&T Global Network, необходимо настроить специальные профайлы.

При подключении к этой сети с помощью Мастера подключения к AT&T Global Network можно настроить профайл соединения PPP по коммутируемой линии с набором номера. Настройка профайла с помощью мастера состоит в заполнении 8 панелей и занимает около 10 минут. Вы можете прервать работу с мастером без сохранения данных в любой момент времени.

Соединение с AT&T могут использовать приложения следующих типов:

- **Почтовая программа**: Позволяет периодически получать почту с помощью единой учетной записи AT&T Global Network и передавать ее в систему для рассылки пользователям Lotus Mail или клиентам, поддерживающим протокол SMTP.
- **Удаленный доступ к сети**: Обеспечивает работу других приложений, поддерживающих удаленный доступ (например, стандартных программ для работы в Internet), совместно с AT&T Global Network.

Работа с профайлом AT&T осуществляется точно так же, как и с любым другим профайлом PPP.

Для применения Мастера подключения к AT&T Global Network необходим один из следующих адаптеров:
- 2699: WAN IOA на две линии
- 2720: PCI WAN/твинаксиальный IOA
- 2721: PCI WAN IOA на две линии
- 2745: PCI WAN IOA на две линии (замена IOA 2721)
- 2771: Двухпортовый WAN IOA со встроенным в первый порт модемом V.90 и стандартным интерфейсом соединений для второго порта. Для применения второго порта адаптера 2771 необходим внешний модем или терминальный адаптер ISDN с соответствующим кабелем.
- 2772: Двухпортовый интегрированный модем V.90 WAN IOA
- 2793/576C: Двухпортовый WAN IOA со встроенным в первый порт модемом V.92 и стандартный интерфейсом соединений для второго порта. Он заменяет модель 2771.
- 2805: 4-портовый WAN IOA со встроенным модемом V.92. Он заменяет модели 2761 и 2772.

Перед запуском Мастера подключения к AT&T Global Network необходимо собрать следующие сведения о системе:
- Сведения об учетной записи AT&T Global (номер учетной записи, ИД пользователя и пароль) для почтовой программы и приложений, использующих удаленный доступ к сети.
- IP-адреса почтового сервера и сервера имен доменов для почтовой программы.
- Имя модема, используемого для соединения по одной линии.

Для запуска Мастера подключения к AT&T Global Network выполните следующие действия:
1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на пункте **Профайлы исходящих соединений** и выберите **Новое подключение к AT&T Global Network**.
3. После запуска Мастера подключения к AT&T Global Network нажмите кнопку **Справка** для получения информации о текущей панели.

Мастера соединений

Для работы с конфигурацией профайла соединения используйте мастер соединения.

Мастер создания модемного соединения

Этот мастер поможет вам последовательно выполнить действия по настройке модемного соединения для доступа к провайдеру или к Intenet. Возможно, для выполнения инструкций мастера вам потребуется получить некоторую информацию от администратора сети или провайдера Internet (ISP). Дополнительная информация о мастере приведена в электронной справке.

IBM Мастер универсального соединения

Этот мастер поможет вам последовательно выполнить действия по настройке профайла соединения с IBM для электронной поддержки клиентов. Электронная поддержка клиентов обеспечивает отслеживание конкретной среды i5/OS и предоставление рекомендаций при возникновении проблем.

Информация, связанная с данной

Универсальное соединение

Настройка групповой стратегии доступа

Папка **Групповые стратегии доступа** раздела Профайлы входящих соединений позволяет настраивать параметры двухточечных соединений для групп удаленных пользователей. Они применяются только для соединений, инициированных удаленной системой, и принятых локальной системой.

Для настройки новой групповой стратегии выполните следующие действия:

1. В System i выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа → Профайлы входящих соединений**.
2. Щелкните правой кнопкой мыши на пункте **Групповые стратегии доступа** и выберите **Создать групповую стратегию доступа**.
3. На вкладке **Общие** задайте имя и описание новой групповой стратегии доступа.
4. Откройте вкладку **Многоканальные соединения** и задайте конфигурацию многоканальных соединений.

   В этой конфигурации несколько физических линий связи объединяются в один канал. Один канал может состоять не более чем из 6 отдельных линий. Поскольку тип линии неизвестен до момента создания соединения, по умолчанию всегда принимается значение 1. Групповую стратегию можно использовать для расширения или ограничения пропускной способности многоканального протокола для отдельного пользователя.

   Значение **Максимальное число линий в наборе** задает максимальное число линий связи в одной логической линии.Максимальное число линий связи не превышает число свободных линий на момент применения стратегии к профайлу PPP.

   Для запрета подключения к системе, не поддерживающей протокол BACP, отметьте переключатель **Не подключаться к системам без поддержки BACP**. Если протокол BACP не поддерживается, то допускается только отдельная линия связи.
5. Для включения одной из следующих опций откройте вкладку **Параметры TCP/IP**:

   Предоставить удаленной системе доступ к другим сетям. Эта опция указывает, разрешена ли пересылка IP. Если она выбрана, то система сможет работать в качестве маршрутизатора для этого соединения. Это позволит пересылать дейтаграммы протокола IP, не предназначенные для данной системы, в другую сеть через эту систему. Если эта опция не отмечена, то протокол IP будет отбрасывать все дейтаграммы удаленной системы, не предназначенные для систем в локальной сети данной системы.

   Пересылку IP можно запретить из соображений защиты. Напротив, ISP обычно разрешает пересылку IP. Обратите внимание, что пересылка дейтаграмм IP будет работать только в том случае, если она разрешена для всей системы. Пересылку дейтаграмм IP для всей системы можно включить на вкладке **Настройка** окна Свойства IPv4.

   Запрашивать сжатие заголовка TCP/IP (VJ). Эта опция указывает, следует ли сжимать заголовки IP-пакетов после установления соединения. Сжатие позволяет повысить пропускную способность соединения, особенно на медленных последовательных линиях. Заголовки сжимаются с применением метода Ван-Якобсона (VJ), описанного в документе RFC 1332. Для соединений PPP согласование о сжатии происходит после создания соединения. Если другая сторона не поддерживает сжатие VJ, то система устанавливает соединение без сжатия.

   Применять фильтрацию IP-пакетов. Эта опция указывает, разрешена ли фильтрация IP-пакетов. Правила фильтрации управляют трафиком IP в сети. Они позволяет отбрасывать пакеты IP в соответствии и указанными правилами. Пакеты фильтруются в зависимости от их заголовков.

Применение групповой стратегии к удаленному пользователю:

После задания свойств нового профайла входящих соединений можно задать групповую стратегию для удаленного пользователя.

Для применения групповой стратегии к удаленному пользователю выполните следующие действия:

1. Нажмите кнопку **Идентификация**, чтобы открыть страницу Идентификация.

2. Нажмите кнопку **Обязательная проверка и идентификация удаленных систем сервером iSeries**.
3. Выберите **Локальная идентификация с помощью контрольного списка**.
4. Если в системе есть контрольный список, выберите его в списке и нажмите **Открыть**. Для создания контрольного списка введите его имя и нажмите **Создать**.
5. Нажмите кнопку **Добавить** для добавления пользователя в контрольный список.
6. В окне Добавить пользователя укажите следующую информацию:
   a. Выберите протокол идентификации, для которого задается имя пользователя.
   b. Введите имя пользователя и пароль.

      Примечание: Из соображений защиты рекомендуется применять разные пароли для пользователей протоколов CHAP, EAP и PAP.
   c. Отметьте переключатель **Применить групповую стратегию к пользователю**, выберите стратегию в списке и нажмите **Открыть**.

   При необходимости групповую стратегию можно изменить.
7. Нажмите **OK** для завершения настройки и возврата к окну свойств PPP.

Ссылки, связанные с данной

“Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23
Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Информация, связанная с данной

Фильтрация IP-пакетов и преобразование сетевых адресов

Применение правил фильтрации IP-пакетов в соединениях PPP

С помощью файла правил фильтрации пакетов можно ограничить доступ пользователя или группы к IP-адресам в локальной сети.

В разделе Правила фильтрации IP-пакетов и преобразование сетевых адресов (NAT) справочной системы Information Center описаны способы создания правил фильтрации IP-пакетов, которые можно применять в профайлах соединений PPP.

Просмотр правил фильтрации IP-пакетов возможно двумя способами:

- Уровень профайла соединения
  1. После задания **Свойств PPP** для **Профайла входящих соединений** откройте окно свойств TCP/IP и нажмите кнопку **Дополнительно**.
  2. Отметьте переключатель **Применять фильтрацию IP-пакетов** и выберите идентификатор фильтра PPP в списке.
  3. Нажмите **OK** для применения фильтрации PPP с этим профайлом соединения.
- Уровень пользователя
  1. Откройте существующую групповую стратегию доступа или создайте новую стратегию.
  2. Откройте страницу Параметры TCP/IP
  3. Отметьте переключатель **Применять фильтрацию IP-пакетов** и выберите идентификатор фильтра PPP в списке.
  4. Нажмите **OK** для применения фильтра PPP.

Ссылки, связанные с данной

“Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов” на стр. 23

Групповые стратегии доступа определяют группы пользователей, устанавливающих соединение, и позволяют задать некоторые общие атрибуты соединения и защиты для всей группы. В сочетании с фильтрацией IP-пакетов это позволяет разрешить или запретить доступ к конкретным IP-адресам в локальной сети.

Включение служб RADIUS и DHCP для профайлов соединений

Здесь приведены действия по включению RADIUS или служб Протокола динамической настройки хостов (DHCP) для профайлов входящих соединений PPP.

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на пункте **Службы удаленного доступа** и выберите **Службы**.
3. Щелкните на вкладке **DHCP-WAN**.Система автоматически включит DHCP (протокол динамической настройки хостов) и определит, какие сервер и агенты DHCP (если они есть) в ней запущены.
4. Для включения служб RADIUS перейдите к вкладке **RADIUS**.
   a. Выберите **Разрешить подключение к серверу RADIUS**
   b. Выберите **Включить идентификацию с помощью RADIUS**.
   c. В зависимости от конфигурации RADIUS, вы можете также выбрать ведение учета соединений и настройку IP-адресов с помощью RADIUS.
5. Нажмите кнопку **Параметры NAS RADIUS** для настройки соединения с сервером RADIUS.
6. Нажмите кнопку **OK**, чтобы вернуться кSystem i Navigator.

Ссылки, связанные с данной

“Сценарий: Идентификация коммутируемых соединений с помощью Сервера сетевого доступа (NAS) RADIUS” на стр. 21
Сервер сетевого доступа (NAS), запущенный в системе может направлять запрос на идентификацию от входящих клиентов на отдельный сервер Службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS). После идентификации сервер RADIUS может управлять IP-адресами пользователей.

Управление PPP

В этом разделе описано управление PPP в системе.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа” на стр. 67
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Задание свойств профайла соединения PPP

При создании профайла соединения в окне Настройка профайла соединения PPP обычно задаются протокол, тип соединения и режим работы соединения.

После задания этих значений появится окно свойств профайла соединений. Содержимое и порядок вкладок окна свойств профайла определяется значениями, введенными на странице Настройка профайла соединения PPP. Окна свойств профайлов входящих и исходящих соединений различаются.

При указании значений в окне Свойства нового профайла PPP можно воспользоваться следующими рекомендациями. Значения свойств зависят от среды и типа настраиваемого соединения. Все опции окна описаны в электронной справке System i Navigator. Дополнительная информация приведена в примерах PPP и процедурах.

Монитор PPP

Здесь приведена информация о том, как просматривать профайл соединения и протокол сеанса с помощью System i Navigator.

О заданиях соединения PPP:

- Управлять отдельными нитями соединений PPP можно с помощью двух контрольных заданий PPP. Эти задания работают в подсистеме QSYSWRK:
  - QTPPPCTL - Основное управляющее задание PPP. Это задание управляет всеми нитями соединений PPP.
  - QTPPPL2TP - Сервер L2TP. Это задание управляет организацией туннелей L2TP и работает только при запущенном профайле L2TP.
- Нити соединения PPP в QTPPPCTL работают от имени пользователя QTCP.
- Задания SLIP работают в подсистеме QSYSWRK с пользовательским профайлом QTCP. Любое задание SLIP относится к одному из двух следующих типов:
  - QTPPDIAL*nn* соответствуют исходящим звонкам, где *nn* - число от 1 до 99.
  - QTPPANS*nnn* соответствуют входящим звонкам, где *nnn* - число от 1 до 999.

Работа с профайлами соединений:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**. Выберите **Профайл исходящих соединений** или **Профайл входящих соединений**.
2. В столбце Профайл щелкните правой кнопкой мыши на имени нужного профайла и выберите одну из следующих опций:
   - **Соединения** - будет показано окно с информацией обо всех соединениях, связанных с профайлом. Эта информация может содержать данные о текущем соединении, о предыдущих соединениях, либо всю эту информацию. Для каждого соединения доступны опции, позволяющие просмотреть вывод заданий и сведения о соединении, протоколы вызовов и протоколы сообщений.
   - **Свойства** - будут показаны параметры соединения.

Просмотр информации о соединении:

1. В окне System i Navigator выберите свою систему и откройте раздел **Сеть → Службы удаленного доступа**. Выберите **Профайл исходящих соединений** или **Профайл входящих соединений**.
2. Для просмотра информации о соединении щелкните в столбце Профайл правой кнопкой мыши на имени любого активного профайла и выберите **Соединения**.

   Будут показаны как текущие, так и предыдущие соединения для этого профайла. В строке состояния показано состояние каждого соединения. Дополнительная информация, такая как ИД подключенного пользователя, ИД нити, локальный и удаленный IP-адреса и имя задания PPP, будет показана в зависимости от состояния каждого задания PPP.
3. Для просмотра вывода заданий, подробной информации о соединении, протоколов вызовов или протоколов сообщений щелкните правой кнопкой мыши на соединении.
4. Для просмотра QTPPPCTL нажмите **Задания**. Для того чтобы показать информацию обо всех нитях соединения, связанных с QTPPPCTL, щелкните правой кнопкой мыши на имени задания и выберите **Вывод на принтер** или **Протокол задания** в окне соединения.
5. Для просмотра подробной информации о соединении нажмите **Сведения**.Эту информацию можно просмотреть только для активных соединений. Окно Сведения позволяет просмотреть дополнительную информацию о конкретном соединении.
6. Для просмотра протоколов вызова нажмите **Протокол вызова**.
7. Для просмотра протоколов сообщений нажмите **Протокол сообщений**.

Работа с выводом PPP в системе:

Для работы с выводом PPP введите команду WRKTCPPTP в системной командной строке:

- Для работы со ВСЕМИ активными заданиями PPP (включая задания QTPPPCTL и QTPPPL2TP) нажмите F14 (Работа с активными заданиями).
- Для работы с выводом конкретного профайла соединения выберите **опцию 8** (работа с выводом) для этого профайла.

- Для вывода на печать конфигурации профайла PPP выберите **опцию 6** (Печать) для этого профайла.Для работы с выводом на принтер воспользуйтесь командой WRKSPLF.

Состояние соединения:

Состояние соединения каждого профайла из списка показано в поле **Состояние** в меню **Сеть → Службы удаленного доступа** после выбора профайла входящего или исходящего соединения. Состояние каждого конкретного соединения можно просмотреть с помощью окна Соединения.

Таблица 10. Основное состояние

Основное состояние	**Описание**
Ожидание запросов на создание соединения	Профайл входящих соединений готов к созданию соединения
Ожидание входящего звонка	Система готова к соединению.
Установление соединения	Устанавливается соединение с удаленной системой
Активно/активные соединения	Соединение установлено и используется заданием
Неактивно	Соединение не используется ни одним заданием
Завершено	Есть информация
Составное соединение в режиме ответа запускает составное соединение в режиме вызова	Составное соединение выполняется
Составное соединение активно	Составное соединение успешно подключено

Таблица 11. Дополнительное состояние

Дополнительное состояние	**Описание**
Инициализация модема	Инициализация модема перед запуском коммутируемого соединения
Ожидание соединения модема	Сервер PPP находится в состоянии ожидания
НАБОР НОМЕРА xxx-xxxx	Номер, набранный клиентом
Определен входящий звонок	Сервер PPP определил входящий модемный звонок
Модем подключен	Квитирование PPP успешно выполнено
Работает	Соединение PPP активно
Связь прекращена	Соединение завершено узлом
Остановлен	Профайл или задание завершены
Ошибка идентификации	Соединения PPP не были установлены из-за ошибки идентификации
Тайм-аут соединения	Соединения PPP не были установлены из-за тайм-аута простоя
Согласование IP-адресов	Соединения PPP не были установлены из-за ошибки согласования IP-адресов
Удаленный модем не отвечает	Соединения PPP не были установлены из-за отсутствия ответа
Отказ от протокола	Соединения PPP не были установлены из-за ошибки согласования Протокола управления сетью (NCP)
Ошибка повтора	Соединение PPP не установлено из-за превышения счетчика повторов
Получено подтверждение на сеанс PPPoE с узла	Согласование PPPoE успешно выполнено
Выполнен вызов L2TP	L2TP получил сообщение

Устранение неполадок PPP

При обнаружении неполадок PPP можно воспользоваться справочной таблицей для сбора информации об ошибках. Эта справочная таблица поможет вам при обнаружении и устранении неполадок соединений PPP.

Важная текущая информация о временных исправлениях программы (PTF) и устранении неполадок приведена на домашней странице TCP/IP дляi5/OS  . На этом Web-сайте доступна информация, дополняющая и заменяющая информацию в этих разделах.

1. Обязательная информация:
   - Тип удаленного хоста, его операционная система и версия системы
   - Версия операционной системы локального хоста i5/OS
   - Все файлы вывода сохранены в очереди вывода с именами профайла
   - Протокол заданий для QTPPPCTL и QTPPPL2TP (профайла L2TP)
   - Сценарий соединения, применяемый в среде
   - Состояние профайла соединения до и после сбоя
2. Рекомендуемая дополнительная информация:
   - Описание линии
   - Профайл соединения

     Параметры профайла можно распечатать с помощью опции 6 задания WRKTCPPTP.
   - Тип и модель модема
   - Командные строки модема
   - Информация о трассировке соединения

Руководство по выполнению задач ITSO V4 TCP/IP для AS/400: More Cool Things Than Ever  описывает следующие неполадки PPP. В ней также приведена подробная информация об их устранении.

Для идентификации неполадок и нахождения решений воспользуйтесь списком в следующей таблице.

Таблица 12. Неполадки PPP из руководства ITSO

Неполадка	Способ устранения
Аппаратная конфигурация модема Неверная конфигурация переключателей и других аппаратных настроек	Убедитесь в том, что модем настроен на нужный тип фреймов. Модем может работать как в *Асинхронном*, так и в *Синхронном* режимах. Дополнительная информация приведена в документации к модему.
Команды AT модема Определение модема, которое вы пытаетесь использовать, отсутствует в списке определений System i Navigator.	Создание нового модема.
Пользователи и пароли PPP При попытке создания соединения PPP выдаются сообщения об ошибках пользователя и пароля.	• Убедитесь в том, что ИД пользователя и пароль введены в верном регистре. • Убедитесь в том, что системы используют один и тот же протокол идентификации. • Если одна из систем использует CHAP, не используйте PAP на другой системе.
Линии связи PPP для запуска нового профайла соединений Идентифицированные линии PPP используются одним и тем же аппаратным ресурсом.	Линии, не использующие в данный момент аппаратный ресурс, необходимо выключать.

Таблица 12. Неполадки PPP из руководства ITSO (продолжение)

Неполадка	Способ устранения
Протокол PPP Ошибки соединений могут возникать из-за неверной конфигурации протокола PPP.	В некоторых ситуациях, если не удается установить соединение между узлами, вам может понадобиться информация о работе нижних уровней протокола PPP. Если протокол PPP или протокол задания PPP не содержит информации о неполадке, то ее можно получить с помощью трассировки связи.

Понятия, связанные с данным

“Настройка модема для работы с PPP” на стр. 56
Модем обеспечивает возможность аналогового соединения (по выделенной или коммутируемой линии). Для аналоговых соединений по Протоколу двухточечной связи (PPP) может применяться внешний модем, внутренний модем или терминальный адаптер Цифровой сети с комплексными услугами (ISDN).

“Настройка нового модема” на стр. 56
Можно настроить новый модем с помощью существующего описания модема или создать описание модема на основании предыдущего описания модема.

Ссылки, связанные с данной

“Связанная информация для Служб удаленного доступа”
Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

Связанная информация для Служб удаленного доступа

Публикации IBM Redbooks и Web-сайты содержат информацию, связанную с Службами удаленного доступа. Файлы PDF можно и просматривать, и печатать.

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic!
- V4 TCP/IP для AS/400: More Cool Things Than Ever

Web-сайты

Для перехода к последним версиям временных исправлений программ (PTF) и свежей информации о настройке PPP и L2TP выберите ссылку PPP на Web-сайтеTCP/IP для i5/OS . На этом Web-сайте доступна информация, дополняющая и заменяющая информацию в этих разделах.

Ссылки, связанные с данной

“Документ в формате PDF для Служб удаленного доступа.” на стр. 1
Файл PDF этой информации можно просмотреть и напечатать.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

© Copyright IBM Corp. 1998, 2008

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Соглашения о лицензии на машинный код или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для того чтобы примеры были максимально наглядными, в них указаны имена людей, а также названия компаний, товарных знаков и продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия на продукты, защищенные авторским правом:

Эта информация содержит примеры приложений на исходном языке, иллюстрирующие приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для интерфейсов, соответствующих той операционной платформе, для которой созданы примеры. Работа примеров не была проверена во всех возможных условиях. По этой причине, IBM не может гарантировать их надежность и пригодность.

Любая копия или часть этих примеров программ, а также произведений, созданных на их основе, должна содержать следующее заявление об авторских правах:

© (название вашей фирмы) (год). Этот код частично создан на основе примеров программ фирмы IBM Corp.
© Copyright IBM Corp. _год или годы_. Все права защищены.

При просмотре данного документа в электронном виде фотографии и цветные иллюстрации могут не отображаться.

Информация об интерфейсе программирования

Сервисы удаленного доступа: публикация о соединениях PPP документирует рекомендуемые интерфейсы программирования, позволяющие писать программы, использующие службы IBM i5/OS.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

AIX
AS/400
eServer
i5/OS
IBM
IBM (логотип)
iSeries
Lotus
OS/400
Redbooks
System i

Adobe, логотип Adobe, PostScript и логотип PostScript являются зарегистрированными товарными знаками или товарными знаками Adobe Systems Incorporated в США и/или других странах.

Linux является зарегистрированным товарным знаком Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

UNIX является зарегистрированным товарным знаком The Open Group в США и/или других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками корпорации Microsoft в Соединенных Штатах и/или других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Напечатано в Дании