IBM

eserver

iSeries

Службы удаленного доступа: Соединения PPP

IBM Confidential

IBM @server

iSeries

Службы удаленного доступа: Соединения PPP

IBM Confidential

Содержание

Часть 1. Службы удаленного доступа: Соединения PPP

Двухточечный протокол (PPP) - это стандарт Internet для передачи данных по последовательным линиям. Это наиболее распространенный протокол, который поддерживается большинством провайдеров Internet (ISP). PPP позволяет отдельным компьютерам получать доступ к сетям, которые, в свою очередь, обеспечивают доступ к Internet. В комплект средств поддержки глобальных сетей (WAN) сервера iSeries входит поддержка PPP TCP/IP.

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

- Новое в версии V5R2 Здесь описаны новые функции Служб удаленного доступа в этом выпуске операционной системы.
- Пункт Как напечатать этот раздел позволяет загрузить и напечатать версию этого документа в формате PDF.

Принципы работы служб удаленного доступа: Соединения PPP

В этих разделах кратко описаны службы удаленного доступа сервера iSeries 400. Приведенные ниже разделы помогут вам при создании в сети среды PPP.

- В разделе **Сценарии PPP** приведены примеры различных реализаций соединения PPP. В каждом сценарии есть указания и примерные значения для настройки соединений PPP.
- В разделе **Принципы работы PPP** описаны основные принципы работы соединений PPP и требования к серверу iSeries 400 для поддержки соединений PPP.
- В разделе **Планирование соединений PPP** описаны основные принципы работы соединений PPP и требования к серверу iSeries 400 для поддержки соединений PPP.

Применение служб удаленного доступа: Соединения PPP

Эти разделы содержат рекомендации по настройке и управлению соединениями PPP на сервере iSeries 400.

- В разделе **Настройка PPP** описаны основные этапы настройки соединения PPP.
- Раздел **Управление PPP** содержит информацию, которую можно использовать в качестве руководства по управлению соединениями PPP.
- В разделе **Устранение неполадок PPP** описаны основные ошибки в работе соединений PPP и приведены ссылки на информацию по их исправлению.

Раздел Дополнительная информация о PPP содержит ссылки на полезную информацию о соединениях PPP на сервере iSeries.

Глава 1. Новое в версии V5R2

В версии V5R2 Навигатор может устанавливать соединения PPP по сети Ethernet (PPPoE), исходящие от сервера iSeries. Для этого применяется новый тип виртуальной линии PPPoE, связанной с физической линией Ethernet. Он позволяет устанавливать соединения PPP с помощью адаптера Ethernet LAN, подключенного к модему DSL. После установления соединения между iSeries и провайдером Internet (ISP) отдельные пользователи локальной сети (LAN) получают доступ к ISP по соединению PPPoE iSeries. Новая функция доступна из меню Профайлы исходящих соединений или из мастера Универсальное соединение.

Дополнительная информация приведена в разделе Подключение сервера iSeries к концентратору PPPoE

Ниже перечислены некоторые изменения в Навигаторе, упрощающие настройку соединений PPP и управление ими:

- Окно настройки DHCP-WAN теперь автоматически опрашивает интерфейс сервера и клиента Протокола динамической настройки хостов (DHCP) для определения IP-адреса интерфейса клиента DHCP-WAN. Для перехода к этому окну диалога выполните следующие действия:
  - Откройте **Сеть > Службы удаленного доступа**
  - Щелкните правой кнопкой мыши на пункте **Службы удаленного доступа**
  - Выберите пункт **Службы**
  - Выберите вкладку **DHCP-WAN**
- Окно диалога Состояние соединений теперь предоставляет дополнительную информацию о соединениях L2TP, L2TP с несколькими транзитными участками, мультиканальных соединениях и соединениях PPP по сети Ethernet, упрощая управление соединениями PPP.
- В панель задач добавлена возможность создания Профайлов исходящих и входящих соединений, а также Групповых стратегий доступа.
- Мастеры Создать удаленное соединение и Универсальное соединение были переименованы соответственно в мастеры Создать удаленное соединение с Internet или ISP и Создать Универсальное соединение IBM.
- Профайлы исходящих соединений могут теперь ″одалживать″ линию PPP и модем, связанные с профайлом входящих соединений, ожидающим входящего звонка. Исходящее соединение ″вернет″ линию PPP и модем профайлу входящего соединения после завершения соединения. Для включения этой функции необходимо выбрать опцию **Включить динамическое разделение ресурсов** на вкладке Модем окна Настройка линии PPP. Настройка линий PPP происходит на вкладке Соединения меню Профайлы входящих и исходящих соединений.
- Свойства пула линий не могут быть изменены, когда пул линий используется; это предотвращает возможные неполадки пула линий.
- Поддержка режимов работы Вызов по запросу и Удаленный набор номера по запросу убрана из меню Профайлы исходящих соединений с помощью L2TP.

Глава 2. Как напечатать этот раздел

Вы можете просмотреть документ или загрузить его версию в формате PDF для последующего просмотра или печати. Для просмотра файлов в формате PDF необходима программа Adobe® Acrobat® Reader. Ее можно загрузить с Web-сайта фирмы Adobe .

Для просмотра или загрузки документа в формате PDF выберите Службы удаленного доступа: Соединения PPP (277 Кб, или около 58 страниц).

Для сохранения файла в формате PDF на рабочей станции с целью последующего просмотра или печати выполните следующие действия:

1. Откройте файл PDF в браузере (щелкните на приведенной выше ссылке).
2. В меню браузера выберите **Файл**.
3. Щелкните на **Сохранить как...**
4. Укажите каталог, в котором вы хотите сохранить документ.
5. Щелкните на **Сохранить**.

Глава 3. Сценарии PPP

Приведенные ниже сценарии помогут вам ознакомиться с основными принципами работы соединений PPP и способами реализации 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.

Сценарий: Подключение сервера iSeries к концентратору PPPoE

Множество провайдеров Internet предоставляют высокоскоростной доступ к Internet по линиям DSL с помощью PPPoE. Сервер iSeries может подключиться к этим провайдерам для обеспечения соединений с высокой пропускной способностью, обладающих всеми преимуществами PPP.

Сценарий: Подключение удаленных клиентов к серверу iSeries

Удаленным пользователям, таким как надомные работники или сотрудники, находящиеся в командировке, часто требуется доступ к сети компании. Этим пользователям можно предоставить доступ к серверу iSeries с помощью соединения PPP.

Сценарий: Подключение локальной сети к Internet с помощью модема

Сети, создаваемые администраторами, как правило, позволяют работникам получать доступ к Internet. Сервер iSeries можно подключить к провайдеру Internet с помощью модема. Клиенты PC, подключенные к сети, будут использовать сервер iSeries в качестве шлюза при доступе к Internet.

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 серверу iSeries в центральном офисе, а другую - к другому серверу iSeries в офисе филиала компании.

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

Сервер сетевого доступа (NAS), запущенный на сервере iSeries, может направлять запрос на идентификацию от входящих клиентов на отдельный сервер RADIUS. После идентификации сервер RADIUS может управлять IP-адресами и портами пользователей.

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.

Сценарий: Применение PPP и DHCP на одном сервере iSeries

Удаленные модемные клиенты могут получить доступ к серверу iSeries в сети компании с помощью соединения PPP. Клиент глобальной сети DHCP на том же сервере iSeries позволяет удаленным пользователям получать динамически присваиваемый IP-адрес с помощью тех же служб, что и пользователи, подключенные по локальной сети.

Сценарий: Профайлы DHCP и PPP на разных серверах iSeries

Из-за физической топологии сети или по соображениям безопасности сетевые службы часто располагаются на разных серверах. Данный сценарий позволяет обойти все трудности, связанные с расположением служб PPP и DHCP на разных серверах. Как и в предыдущем сценарии, удаленные пользователи могут устанавливать модемное соединение с сервером и получать доступ к сети компании.

Сценарий: PPP и VPN: Дополнительный туннель L2TP, защищенный VPN

Офис филиала компании можно подключить к основному офису с помощью протокола L2TP. В дополнительном туннеле L2TP создается виртуальная линия связи PPP. Фактически L2TP позволяет расширить корпоративную офисную сеть, сделав сеть филиала частью корпоративной подсети. Протокол VPN позволяет защитить поток данных в туннеле L2TP.

Сценарий: Подключение сервера iSeries к концентратору PPPoE

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 сервер iSeries.

Рисунок 1. Подключение сервера iSeries к ISP с помощью PPPoE

Решение: Вы можете установить соединение PPPoE с локальным ISP через сервер iSeries. Сервер iSeries использует новый тип виртуальной линии PPPoE, связанной с физической линией Ethernet с адаптером Ethernet 2838. Этот тип виртуальных линий поддерживает сеансы PPP по локальной сети Ethernet, подключенной к модему DSL, который является шлюзом к удаленному ISP. Таким образом пользователи, подключенные к локальной сети, получают высокоскоростной доступ к Internet с помощью соединения PPPoE сервера iSeries. После установления соединения между iSeries и провайдером Internet (ISP) пользователи LAN получают доступ к ISP по соединению PPPoE iSeries,

используя IP-адрес сервера iSeries. С целью обеспечения дополнительной защиты для виртуальной линии PPPoE можно определить правила фильтрации, ограничивающие входящий поток данных из Internet.

Образец конфигурации:

1. Настройте устройство, через которое устанавливается соединение с ISP.
2. Настройте профайл исходящего соединения на сервере iSeries.

   Убедитесь, что была введена следующая информация:

   - **Тип протокола**: PPP
   - **Тип соединения**: PPP через Ethernet
   - **Режим работы**: Вызов
   - **Конфигурация линии связи**: отдельная 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. Откройте страницу **Соединение**. Выберите **имя виртуальной линии PPPoE**, соответствующее имени этого профайла соединения. После выбора линии в Навигаторе появится окно ее свойств.
   a. На странице **Общие** введите описание виртуальной линии PPPoE.
   b. Откройте страницу **Линия**. 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**. Навигатор перейдет к окну свойств линии Ethernet. **Примечание:** Для работы PPPoE необходим адаптер Ethernet 2838.
      1) На странице **Общие** введите описание линии Ethernet и убедитесь в том, что линия использует предполагаемые аппаратные ресурсы.
      2) Откройте страницу **Линия**. Введите свойства физической линии Ethernet. Дополнительная информация приведена в соответствующем разделе электронной справки и в документации по карте Ethernet.
      3) Перейдите на страницу **Прочие**. 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.
5. Если вы хотите, чтобы сервер iSeries идентифицировал себя при подключении к ISP, либо чтобы сервер iSeries идентифицировал удаленный сервер, перейдите на страницу **Идентификация**. Дополнительная информация приведена в разделе Идентификация систем.
6. Перейдите на страницу **Параметры TCP/IP** и укажите параметры обработки IP-адресов для этого профайла соединения. Для того чтобы пользователи LAN могли подключаться к ISP с помощью IP-адресов, выделенных серверу iSeries, выберите пункт **Скрыть адреса (Полная маскировка)**.
7. Откройте страницу **DNS** и введите IP-адрес сервера DNS, предоставленный провайдером.
8. Если вы хотите указать подсистему для выполнения задания соединения, перейдите на страницу **Прочие**.
9. Для создания профайла нажмите **OK**.

Информация об ограничении доступа пользователей к внешним IP-адресам и ресурсам iSeries приведена в разделах Фильтрация IP-пакетов и Групповые стратегии доступа.

Сценарий: Подключение удаленных клиентов к серверу iSeries

Ситуация: Вы - администратор сети компании, и в ваши обязанности может входить обслуживание как сервера iSeries, так и сетевых клиентов. В этом случае вам наверняка понравится возможность устранять неполадки, не приходя в офисе компании, например, из дома. Допустим, что офис компании не подключен к сети Internet, и подключаться к серверу iSeries можно с помощью соединений PPP. Кроме того, единственным модемом в системе является модем 7852-400 ECS, и его можно применить для создания соединения.

Рисунок 2. Подключение удаленных клиентов к серверу iSeries

Возможные действия: Домашний PC можно подключить к системе iSeries с помощью соединения PPP и модема. Поскольку для создания соединений PPP этого типа применяется модем ECS, то необходимо убедиться, что модем настроен для работы как в синхронном, так и в асинхронном режимах. На рисунке показан сервер iSeries с двумя службами PPP, подключенный к локальной сети с двумя PC. Удаленный пользователь может создать модемное соединение с сервером iSeries, идентифицировать себя и стать пользователем рабочей сети (`192.168.1.0`). В этом случае проще всего будет присвоить удаленному клиенту статический IP-адрес.

Для идентификации на сервере iSeries удаленный пользователь применяет CHAP-MD5. Применение MS_CHAP на сервере iSeries 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 ECS не поддерживает несколько параллельных соединений. Информация о том, что необходимо для одновременного подключения нескольких удаленных клиентов приведена в разделе планирования аппаратного и программного обеспечения.

Образец конфигурации:

1. Настройте удаленный доступ к сети и создайте модемное соединение с удаленным PC.
2. Настройте профайл входящего соединения на сервере iSeries.

   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. Откройте страницу **Соединение**. Выберите **Имя линии** или создайте новую линию с помощью кнопки **Создать**.
   a. На странице **Общие** выберите существующий аппаратный ресурс и присвойте параметру Обработка кадров значение **Асинхронная**.
   b. Откройте страницу **Модем**. В списке имен модемов выберите модем **IBM 2772**.
   c. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
5. Откройте страницу **Идентификация**.
   a. Выберите значение **Обязательная проверка и идентификация удаленных систем**.
   b. Выберите **Идентификация с помощью контрольного списка** и добавьте нового удаленного пользователя в контрольный список.
   c. Выберите опцию **Разрешить шифрование паролей (CHAP-MD5)**.
6. Откройте страницу **Параметры TCP/IP**.
   a. Задайте локальный IP-адрес `192.168.1.1`.
   b. Для удаленных адресов выберите **Фиксированный IP-адрес** с начальным адресом `192.168.1.11`.
   c. Выберите опцию **Предоставить удаленной системе доступ к другим сетям**.
7. Для создания профайла нажмите **OK**.

Сценарий: Подключение локальной сети к Internet с помощью модема

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

Рисунок 3. Подключение локальной сети к Internet с помощью модема

Возможные действия: Для подключения сервера iSeries к провайдеру Internet (ISP) можно использовать модем ECS или любой другой совместимый модем. Для подключения сервера к ISP с помощью соединения PPP необходимо создать профайл инициатора соединения PPP.

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

При подключении системы iSeries и 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.

Если для этого типа соединений PPP применяется модем ECS, то его необходимо настроить для работы в асинхронном режиме. В зависимости от объема данных, получаемых и отправляемых в

Internet, полоса пропускания соединения может стать недостаточной. Дополнительная информация об увеличении пропускной способности соединения приведена в разделе планирование.

Образец конфигурации:

1. Настройте профайл исходящего соединения на сервере iSeries.

   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. Откройте 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. Откройте 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 ISP нажмите кнопку **Добавить** и введите номер телефона провайдера. Убедитесь в том, что номер введен с правильным префиксом.
5. Откройте страницу **Идентификация** и выберите опцию **Разрешить удаленной системе идентификацию сервера iSeries**. Выберите протокол идентификации и введите имя пользователя и пароль.
6. Откройте страницу Параметры 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 Навигаторе 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 на сервер iSeries.

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

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 4. Подключение сети филиала компании к основной сети с помощью модема

Возможные действия: Подключить одну локальную сеть к другой можно с помощью соединения PPP между двумя серверами iSeries, как это показано на рисунке выше. Инициатором соединения

должен стать сервер в удаленном офисе. Для этого необходимо настроить профайл исходящего соединения на удаленном сервере iSeries и профайл входящего соединения на сервере 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.

Образец конфигурации:

1. Настройте профайл исходящего соединения на сервере iSeries.

   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. Откройте 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. Откройте 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 iSeries нажмите кнопку **Добавить** и введите номер телефона, к которому подключена удаленная система iSeries. Убедитесь в том, что номер введен с правильным префиксом.
5. Откройте страницу **Идентификация** и выберите опцию **Разрешить удаленной системе идентификацию системы iSeries**. Выберите опцию **Запрашивать зашифрованный пароль (CHAP-MD5)** и введите требуемое имя пользователя и пароль.
6. Откройте страницу **Параметры 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** на сервере iSeries, расположенном 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. Откройте 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. Откройте страницу **Модем**. В списке имен модемов выберите имя применяемого модема.
   c. Для возврата на страницу свойств нового профайла PPP нажмите **OK**.
10. Откройте страницу **Идентификация**.
   a. Отметьте переключатель **Обязательная проверка и идентификация удаленных систем**.
   b. Добавьте нового удаленного пользователя в контрольный список.
   c. Задайте обязательную идентификацию CHAP-MD5.
11. Откройте страницу **Параметры TCP/IP**.
   a. В качестве локального IP-адреса укажите IP-адрес интерфейса сервера в центральном офисе (192.168.1.1).
   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 сервер iSeries в качестве шлюза, необходимо выбрать опцию **Пересылка IP**.
12. Нажмите **OK** для создания профайла входящего соединения.

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

Ситуация: Удаленные пользователи подключаются по коммутируемому соединению к корпоративной сети через два сервера iSeries. Вы хотите выполнять идентификацию, обслуживание и учет централизованно, чтобы один сервер обрабатывал запросы на проверку ИД и паролей пользователей и определял их IP-адреса.

Рисунок 5. Идентификация коммутируемых соединений с помощью сервера RADIUS

Решение: Когда пользователь отправляет запрос на подключение, Сервер сетевого доступа (NAS), запущенный на серверах iSeries, 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 на iSeries.

Образец конфигурации:

1. В Навигаторе откройте **Сеть**, щелкните правой кнопкой мыши на пункте **Службы 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 iSeries, через который подключен сервер RADIUS.
   b. В поле **IP-адрес сервера** введите IP-адрес сервера RADIUS.
   c. В поле **Пароль** введите пароль, по которому сервер iSeries идентифицирует себя на сервере RADIUS.

d. В поле **Порт** введите порт сервера iSeries, через который подключен сервер RADIUS. Введите порт 1812 для сервера идентификации или 1813 - для сервера учета.

6. Нажмите **OK**.
7. В Навигаторе откройте **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 (EAP, PAP или CHAP-MD5). Этот протокол также должен применяться сервером RADIUS. Дополнительная информация приведена в разделе Идентификация систем.
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 сервер iSeries 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.

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

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 серверу.

Рисунок 6. Применение параметров соединения к коммутируемым соединениям на основе групповых стратегий

Решение: 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″. Эти правила фильтрации разрешат доступ к службам HTTP, FTP и Telnet, но запретят доступ ко всем прочим службам и данным TCP/IP через сервер iSeries. 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 сервера iSeries 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.

Образец конфигурации:

1. Создайте идентификатор фильтра PPP и правила фильтрации IP-пакетов для данной групповой стратегии доступа. Дополнительная информация о фильтрации IP-пакетов приведена в разделе Правила обработки IP-пакетов (Фильтрация и Преобразование сетевых адресов (NAT)).
   a. В Навигаторе откройте **Сеть > Службы удаленного доступа**.
   b. Щелкните на пункте **Профайлы входящих соединений**, щелкните правой кнопкой мыши на профайле для данного соединения и выберите пункт **Свойства**.
   c. Выберите вкладку **Параметры TCP/IP** и нажмите **Дополнительно**.
   d. 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.
   e. 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

FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR =  %
        * DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * 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 = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. 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 введите

      ```
      permited_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 = permited_services SET = services_rules
      ```

g. Сохраните изменения и закройте меню. Если впоследствии эти изменения потребуется отменить, введите в текстовом интерфейсе следующую команду:

```
RMVTCPTBL
```

Эта команда удалит все правила фильтрации и NAT (Преобразование сетевых адресов) на сервере.

h. 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. Подробное описание опций Групповых стратегий доступа приведено в разделе Настройка групповой стратегии доступа.
   a. В Навигаторе откройте **Сеть > Службы удаленного доступа > Профайлы входящих соединений**.
   b. Щелкните правой кнопкой мыши на значке Групповые стратегии доступа и выберите Создать групповую стратегию доступа. Навигатор 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 коммутируемыми соединениями.
   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.

Дополнительная информация об идентификации пользователей в соединениях PPP приведена в разделе Идентификация систем.

Глава 4. Принципы работы PPP

Двухточечный протокол (PPP) применяется для соединения сервера iSeries с удаленными сетями, клиентскими PC, другими серверами iSeries или провайдером Internet (ISP). Для успешной работы с протоколом необходимо знать как возможности самого протокола, так и особенности его поддержки в iSeries. Дополнительная информация приведена в следующих разделах:

Что такое PPP?
Двухточечный протокол (PPP) - это протокол TCP/IP, применяемый для соединения двух компьютерных систем. Более подробное описание приведено ниже в этом разделе.

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.

Групповые стратегии доступа
Эти стратегии определяют набор атрибутов соединения и защиты для группы пользователей. Информация о том, как создавать такие стратегии, приведена ниже в этом разделе.

Что такое PPP?

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 - это стандартный протокол Internet. Это наиболее распространенный протокол, который поддерживается большинством провайдеров Internet (ISP). С помощью PPP вы можете подключиться к провайдеру, который в свою очередь, предоставит вам доступ к Internet.

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 о RFC приведена на сайте http://www.rfc-editor.org.

- RFC1661 Point-to-Point Protocol
- RFC1662 PPP on HDLC-like framing
- RFC1994 PPP CHAP

Профайлы соединений

В версии V5R2 применяется два типа профайлов, определяющих параметры для соединения PPP или набора соединений.

- **Профайлы исходящих соединений** - это профайлы двухточечных соединений, которые устанавливаются локальным сервером iSeries с удаленной системой. С помощью этого объекта можно настраивать исходящие соединения.
- **Профайлы входящих соединений** - это профайлы двухточечных соединений, которые удаленные системы устанавливают с локальным сервером iSeries. С помощью этого объекта можно настраивать входящие соединения.

Профайл соединения задает способ работы соединения PPP. Профайл соединения содержит ответы на следующие вопросы:

- Какой протокол будет применяться этим соединением? (PPP или SLIP)
- Должен ли сервер iSeries устанавливать соединение с удаленным компьютером (быть инициатором)? Должен ли сервер iSeries ожидать вызова удаленной системы (быть отвечающей стороной)?
- Какая линия связи будет применяться этим соединением?
- Каким образом сервер iSeries должен определять IP-адрес?
- Каким образом сервер iSeries должен идентифицировать удаленную систему? Где должна храниться идентификационная информация сервера iSeries?

Профайл соединения содержит информацию о следующих параметрах соединения:

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

Сервер iSeries хранит информацию о настройке соединений в профайле соединения. Эта информация позволяет серверу iSeries 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
  — L2TP (виртуальная линия)
  — PPPoE (виртуальная линия)

  Службы PPPoE применимы только для профайлов входящих соединений.
- **Режим работы**. Возможные режимы работы зависят от типа соединения. Информация приведена в следующей таблице:

  Информация о профайлах исходящих соединений приведена в следующей таблице:

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

Таблица 1. Возможные режимы работы для входящих соединений (продолжение)

Тип соединения	Возможные режимы работы
Двухточечное соединение (PPP) по Ethernet	Вызов

Информация о профайлах входящих соединений приведена в следующей таблице:

Таблица 2. Возможные режимы работы для входящих 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
  — Линия ISDN

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

Поддержка групповых стратегий

Поддержка групповых стратегий позволяет администраторам сети определять стратегии управления ресурсами для групп пользователей и позволяет связывать с отдельными пользователями, входящими в сеть с помощью сеансов PPP или L2TP, стратегии управления доступом. Основой этого способа является разделение всех пользователей на категории, для каждой из которых создается отдельная стратегия. Каждая групповая стратегия позволяет 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.

Пример приведен в разделе Сценарий: Управление доступом пользователей к ресурсам с помощью Групповых стратегий доступа и Фильтрации IP-адресов.

Глава 5. Планирование соединений PPP

Создание и администрирование соединений PPP требует хорошего знания как различных способов установления соединений PPP на сервере iSeries, так и широкого набора вариантов построения сети и организации защиты. Информация о возможных вариантах и требованиях к iSeries для установления соединений PPP приведена в следующих разделах.

Требования к программному и аппаратному обеспечению
Соединения PPP поддерживаются начиная с версии Навигатора V4R4. Список других требований приведен в этом разделе.

Альтернативные способы соединения
В iSeries поддерживаются соединения PPP, устанавливаемые с помощью различных носителей, начиная с аналоговых или цифровых телефонных линий и заканчивая выделенными полностью или частично соединениями T1. Описания поддерживаемых соединений приведены в этом разделе.

Необходимое оборудование
Соединения PPP на серверах iSeries могут устанавливаться с помощью модемов, адаптеров терминалов ISDN, адаптеров Token-Ring, адаптеров Ethernet и устройств CSU/DSU. Информация о поддерживаемом аппаратном обеспечении приведена в этом разделе.

Обработка IP-адресов
Для соединений PPP предусмотрено несколько различных вариантов присвоения IP-адресов и фильтрации IP-пакетов. Описание этих опций приведено в этом разделе.

Идентификация систем
Сервер iSeries может выполнять идентификацию в коммутируемых соединениях либо с помощью контрольного списка и паролей, либо с помощью сервера RADIUS. Кроме того, он предоставляет идентификационные данные тем системам, к которым он подключается. Описание опций идентификации приведено в этом разделе.

Полоса пропускания
Сервер iSeries поддерживает мультиканальный протокол для соединений PPP. Это позволяет использовать несколько аналоговых телефонных линий для одного соединения с целью увеличения пропускной способности. Обзор данной поддержки приведен в этом разделе.

Требования к программному и аппаратному обеспечению

Для создания среды PPP необходимы как минимум два компьютера, поддерживающие этот протокол. Один из этих компьютеров, сервер iSeries, может быть как инициатором, так и обработчиком соединения. Для обеспечения доступа удаленных систем сервер iSeries должен соответствовать следующим требованиям:

- **Навигатор** выпуска V4R4 или выше с поддержкой TCP/IP
- Один или два профайла 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 **iSeries Access для Windows (95/98/NT/Millenium/2000/XP)** с Навигатором.
- Сетевой 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)

  - 2750: PCI ISDN V.90 Basic Rate Interface U IOA (2-проводной интерфейс)
  - 2751: PCI ISDN V.90 Basic Rate Interface U IOA (4-проводной интерфейс)
  - 2761: 8-портовый IOA аналогового модема
  - 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
  - 2838: Адаптер Ethernet для соединений PPPoE.
  - 2793: Двухпортовый WAN IOA со встроенным в первый порт модемом V.92 и стандартным интерфейсом соединений для второго порта. Для применения второго порта адаптера 2793 необходим внешний модем или терминальный адаптер ISDN с соответствующим кабелем. Он заменяет модель IOA 2771.
  - 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 RS232 или совместимый с ним.
- В зависимости от типа линии и соединения вам потребуется следующее оборудование:
  - внешний или внутренний модем, 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.

Альтернативные способы соединения

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 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
- Цифровые службы и DDS
- Коммутируемые линии-56
- ISDN
- T1/E1 и раздельный T1
- Frame Relay
- Поддержка туннелей L2TP для соединений PPP
- Поддержка PPPoE (DSL) для соединений PPP

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 RS232 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.

Цифровые службы и DDS

Цифровые службы

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.

DDS

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 таких случаях наиболее выгодным решением проблемы может стать Коммутируемая линия-56. 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.

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 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.

ISDN

Как и линии типа Коммутируемая линия-56, ISDN позволяет устанавливать соединения на основе коммутируемых цифровых линий. В отличие от других служб, 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 RS232, 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. Эта новая технология позволяет терминальным адаптерам выполнять роль цифрового сервера для клиентов со скоростью 56 Кбит/с (X2/56Flex).

Как правило, подключение к терминальному адаптеру ISDN с помощью последовательного интерфейса RS232 позволяет передавать данные на скоростях до 230.4 Кбит/с. Тем не менее, скорость передачи данных сервера iSeries в бодах по асинхронному соединению с интерфейсом RS232 не может превышать 115.2 Кбит/с. К сожалению, скорость передачи данных ограничена значением 11.5 Кбайт/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 синхронную передачу данных с помощью интерфейса RS232 на скорости до 128 Кбит/с, однако этот параметр сервера iSeries ограничен значением 64 Кбит/с.

Сервер iSeries поддерживает асинхронную передачу 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 RS232 в интерфейс V.35, но эта функция пока не реализована в сервере iSeries. 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.

T1/E1 и раздельный T1

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 PBX 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 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 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 T-1 (1.544 Мбит/с) и T-3 (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 T-1. (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. С помощью туннелей L2TP можно разделить точку физического подключения к сети от точки логического доступа к сети, поэтому L2TP называют виртуальным соединением PPP. Протокол L2TP описан в документе RFC2661. Дополнительная информация по RFC приведена на сайте http://www.rfc-editor.org. Туннель может относиться ко всему сеансу PPP, либо только к первому сегменту двухсегментного сеанса. Это описывается с помощью четырех различных моделей туннелей:

- Дополнительный туннель
- Основной туннель - входящий вызов
- Основной туннель - удаленный набор номера
- Транзитное соединение L2TP.

Дополнительный туннель

Дополнительный туннель создается пользователем, как правило, с помощью клиента L2TP. Поэтому пакеты L2TP будут отправляться пользователем провайдеру и пересылаться на 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. Пакеты PPP будут отправляться провайдеру (LAC), а после инкапсуляции в пакеты L2TP пересылаться LNS по туннелю. В этом случае провайдер должен поддерживать протокол L2TP. В этой модели туннель действует только на участке сеанса PPP от провайдера до LNS.

Основной туннель - удаленный набор номера

В этой модели локальный шлюз (LNS) создает туннель до провайдера (LAC) и дает ему указание вызвать отвечающего клиента 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 LAC и 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. В некоторых случаях достижимы скорости до 2 Мбит/с - в 30 и более раз выше, чем у самых современных модемов. PPPoE обозначает Двухточечный протокол по Ethernet. Двухточечный протокол (PPP) обычно применяется для последовательных соединений, таких как коммутируемые соединения через модем. Многие провайдеры DSL Internet теперь применяют PPP по Ethernet из-за предусмотренных в нем функций входа в систему и защиты. Что такое модем DSL? ″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). DSL считается следующим поколением модемных технологий. Хотя модемы DSL схожи с обычными аналоговыми модемами, они обеспечивают гораздо большую пропускную способность.

Необходимое оборудование

Для создания среды PPP можно использовать три типа коммуникационного оборудования.

- Модемы
- Устройства CSU/DSU
- Терминальные адаптеры ISDN
- Адаптеры Ethernet 2838 (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.

Сервер iSeries содержит готовые конфигурации для большого числа модемов, однако при необходимости вы можете добавить новую модель с помощью Навигатора. 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 из комплекта поставки 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 сервером iSeries. В более старых системах в качестве модема ECS применялся внешний модем IBM 7852-400. В новых системах роль модема ECS выполняют внутренние модемы 2771 или 2772.

Устройства 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.

Терминальные адаптеры ISDN

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 на сервере iSeries:

- В разделе Рекомендуемые терминальные адаптеры ISDN описаны наиболее подходящие для системы адаптеры.
- В разделе Информация о некоторых терминальных адаптерах ISDN приведена краткая информация о различных терминальных адаптерах ISDN, которые были протестированы при работе с сервером iSeries.

Для настройки терминального адаптера выполните следующие действия:

1. В Навигаторе выберите свой сервер 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. 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.

Настройка этих параметров с помощью Навигатора описана в разделе Настройка терминального адаптера ISDN.

Рекомендации по выбору терминального адаптера ISDN

В качестве внешнего терминального адаптера (модема) 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 как для входящих, так и для исходящих звонков. 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 сервером iSeries.** Courier I самостоятельно идентифицирует удаленный терминальный клиент по протоколу CHAP, а для идентификации соединения с локальным сервером iSeries применяет Протокол идентификации по паролю (PAP). Таким образом, секретный ответ PAP не передается по соединению ISDN.
- **Соединения, инициируемые удаленной системой.** Courier I требует от вызывающей стороны идентификации по протоколу CHAP, если такая идентификация (в соответствии с конфигурацией входящих звонков) необходима в системе iSeries. Если система iSeries 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

серверу iSeries 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 iSeries значением в 115.2 Кб/с.

Переходник от V.35 к RS-232 также поставляется фирмой Black Box Corporation, номер заказа - FA-058.

Убедитесь в том, что скорость передачи данных по линии V.35 в системе iSeries установлена равной 230.4 Кбит/с.

Информация о некоторых терминальных адаптерах ISDN

Перечисленные ниже терминальные адаптеры более не используются. Их рекомендуется применять только для исходящих удаленных соединений ISDN с сервера iSeries.

3Com Impact IQ ISDN:

Этот терминальный адаптер не рекомендуется применять в системе iSeries 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 iSeries на скоростях, превышающих 115200 бит/с.
- Он не поддерживает протокол идентификации CHAP. Несмотря на это, команда S84=0 позволяет выполнять идентификацию CHAP в системе iSeries.
- Система iSeries 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 в системе iSeries 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 iSeries на скоростях, превышающих 115200 бит/с.
- Он не поддерживает протокол идентификации CHAP. Несмотря на это, команда @M2=C позволяет выполнять идентификацию CHAP в системе iSeries.
- 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 системы iSeries, что снижает производительность при работе по многоканальному протоколу PPP. Это приводит к падению производительности при отправке сервером iSeries данных по многоканальному соединению PPP.

Обработка IP-адресов

Соединения PPP предоставляют несколько вариантов обработки IP-адресов в зависимости от типа профайла соединения, позволяющего функциям управления IP-адресами для соединений PPP ″органично″ работать в сетевой архитектуре. Информация о том, как определить схему IP-адресов для вашей сети, приведена в следующих разделах:

- DHCP

  DHCP (протокол динамической настройки хостов) может централизованно управлять присвоением IP-адресов в вашей сети. Здесь описаны настройка и управление службами DHCP в вашей сети.
- DNS

  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.
- BOOTP

  BOOTP позволяет связать клиентские рабочие станции с сервером iSeries и присвоить им IP-адреса. Здесь описаны настройка и управление службами BOOTP в вашей сети.
- Фильтрация IP-пакетов

  Создание файла правил фильтрации IP-пакетов позволяет ограничить доступ пользователей и групп к конкретным IP-адресам. Раздел описывает поддержку фильтрации IP-пакетов и ее применение в локальной сети.

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 адресами. Этот способ лучше всего подходит для установления временного соединения между двумя офисами.

Существует еще один способ, называемый маскировкой IP-адресов. Например, если сервер iSeries подключен к Internet через провайдера, то системы в сети, подключенной к серверу, могут получить доступ к Internet. В этом случае сервер iSeries ″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 сервера iSeries. Для того, чтобы весь поток данных от систем в сети отправлялся на сервер iSeries, необходима небольшая дополнительная настройка маршрутизации как на пользовательских системах, так и на сервере iSeries, на котором необходимо будет включить опцию ″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 сервера iSeries. Этот адрес будет идентификатором сервера iSeries в соединении 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 iSeries.

Таблица 3. 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 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.

Таблица 3. Опции присвоения IP-адреса для профайла входящих соединений (продолжение)

Опция	Описание
Определять дополнительные IP-адреса на основе ИД пользователя удаленной системы	Эта опция позволяет определять 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 сервер iSeries попытается определить, существует ли IP-адрес, заданный специально для этого пользователя. Если этот адрес существует, то при создании соединения будет использован именно этот адрес, маска подсети и набор дополнительных маршрутов. Если адрес не указан, то по умолчанию будет выбран фиксированный IP-адрес или следующий свободный IP-адрес из пула адресов.
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 iSeries должны правильно настроить маршрутизацию IP-адресов, чтобы клиент мог получить доступ ко всем IP-адресам из локальной сети, которой принадлежит система iSeries.

Фильтрация IP-пакетов

Фильтрация IP-пакетов позволяет ограничить доступ отдельного пользователя к различным службам при работе этого пользователя в сети. Пакеты фильтруются на основе получателя этих пакетов. 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 Навигатора Правила фильтрации IP-пакетов. Дополнительная информация приведена в разделе Правила фильтрации IP-пакетов справочной системы Information Center.

В соединениях L2TP для защиты сетевого потока необходимо применять виртуальную частную сеть (VPN) с фильтрацией IPSEc. Дополнительная информация приведена в разделе VPN справочной системы Information Center.

Идентификация систем

Соединения PPP с сервером iSeries предусматривают несколько вариантов идентификации как удаленных клиентов, подключающихся к iSeries, так и соединений с провайдером Internet (ISP) или с другим сервером, к которому подключается iSeries. Сервер iSeries поддерживает несколько способов работы с идентификационной информацией: от применения простых контрольных списков на сервере iSeries, содержащих имена и пароли всех пользователей с правами доступа, до поддержки серверов RADIUS, хранящих подробную идентификационную информацию обо всех пользователях сети. Сервер iSeries также поддерживает несколько вариантов шифрования ИД и паролей пользователей: от простой смены паролей до поддержки маскирования CHAP-MD5. Вы можете задать параметры идентификации, включая ИД и пароль, идентифицирующие сервер iSeries в исходящих соединениях, на вкладке **Идентификация** профайла соединения в Навигаторе.

Дополнительная информация о работе с контрольной и идентификационной информацией приведена в следующих разделах:

- Служба RADIUS
- Контрольный список

Дополнительная информация о поддерживаемых протоколах идентификации паролей приведена в следующих разделах:

- Протокол идентификации с квитированием связи по вызову (CHAP-MD5)
- Протокол PAP
- Протокол EAP

CHAP-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 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.

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 RAS на уровне все возрастающих требований защиты с помощью модулей сторонних производителей. EAP защищает защищенные VPN от взломщиков, применяющих основные типы атак и подбор пароля. EAP - это дальнейшее развитие протоколов PAP и CHAP.

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

В настоящее время сервер iSeries поддерживает только версию EAP, которая эквивалентна протоколу CHAP-MD5. Однако при применении службы RADIUS вы сможете применять описанные выше схемы идентификации.

PAP

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 CHAP.

Обзор RADIUS

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. Сервер iSeries, 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 (серверу iSeries) предоставлять удаленным пользователям необходимые услуги.

Если сервер RADIUS недоступен, то сервер iSeries 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. Это могут быть файлы паролей UNIX, Kerberos, коммерческая система защиты или даже собственная система защиты. Сервер RADIUS отправляет серверу iSeries информацию о службах, к которым пользователю разрешен доступ, например его IP-адрес. Запросы об учетных записях сервер RADIUS обрабатывает схожим 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. Пример конфигурации сервера RADIUS приведен в сценарии Идентификация коммутируемых соединений с помощью сервера RADIUS.

Контрольный список

В контрольном списке хранятся имена 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**.

Дополнительная информация приведена в соответствующем разделе электронной справки.

Полоса пропускания - многоканальные соединения

Иногда для выполнения определенных задач возникает потребность во временной дополнительной полосе пропускания. В этих случаях 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 RFC1990. Дополнительная информация приведена по адресу http://www.rfc-editor.org.

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 RFC2125 описан как протокол BAP, так и протокол BACP.

Глава 6. Настройка PPP

Перед созданием соединения PPP необходимо настроить среду PPP. В этих разделах приведена информация по настройке среды PPP:

- Создание профайла соединения
- Настройка модема
- Настройка удаленного PC
- Настройка доступа к Internet с помощью AT&T Global Network
- Мастеры соединений
- Настройка групповой стратегии доступа
- Применение правил фильтрации IP-пакетов в соединении PPP
- Включение служб RADIUS и DHCP для профайлов входящих соединений PPP

Создание профайла соединения

Для создания соединения PPP между двумя системами необходимо в первую очередь создать профайл соединения на сервере iSeries. 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 двухточечных соединений, инициируемых сервером iSeries (локальная система). Это профайлы соединений PPP, отвечающей стороной у которых является удаленная система.
- **Профайлы входящих соединений** - профайлы двухточечных соединений, инициируемых удаленной системой. Это профайлы соединений PPP, отвечающей стороной у который является сервер iSeries (локальная система).
- **Модемы**

Для создания профайла соединения выполните следующие действия:

1. В Навигаторе выберите свой сервер и откройте раздел **Сеть–> Службы удаленного доступа**.
2. Выберите одну из следующих опций:
   - Для того чтобы сделать сервер iSeries инициализатором модемных соединений, щелкните правой кнопкой мыши на пункте **Профайлы исходящих соединений**.
   - Для того чтобы разрешить входящие модемные соединения на сервере iSeries, щелкните правой кнопкой мыши на пункте **Профайлы входящих соединений**.
3. Выберите **Новый профайл**.
4. На странице **Настройка нового профайла соединения PPP** выберите тип протокола.
5. Укажите способ выбора режима.
6. Выберите пункт конфигурация линии связи.
7. Нажмите **OK**.

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

Тип протокола: PPP или SLIP

Какой тип протокола следует выбрать при создании двухточечного соединения?

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

PPP постепенно вытесняет SLIP с рынка двухточечных соединениях. 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 все еще применяется и поддерживается сервером iSeries. 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
   - L2TP (виртуальная линия)
   - Линия 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

Выберите этот тип соединения, если для подключения по телефонной линии применяется одно из следующих устройств:

- Модем (внутренний или внешний)
- Внутренний адаптер ISDN Basic Rate Interface
- Внешний терминальный адаптер ISDN

Коммутируемая линия может работать в следующих режимах:

- **Ответ**

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

- **Набор номера**

  Выберите этот режим работы для набора сервером iSeries номера удаленной системы.

- **Набор номера по запросу (только набор номера)**

  Выберите этот режим работы для автоматического набора сервером iSeries 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 сервера iSeries на вызовы выделенной удаленной системе. Этот режим работы также позволяет серверу iSeries вызывать удаленную систему при получении от нее пакетов TCP/IP. Если на обеих сторонах соединения работают серверы iSeries 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 этот тип соединения, если сервер iSeries соединен 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 серверу iSeries по выделенной линии. Этот режим работы предназначен для профайла ответа выделенной линии.

- **Вызов**

  Выберите этот режим работы для доступа сервера iSeries 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 системой iSeries 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 серверу iSeries по туннелю L2TP.

- **Вызов**

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

- **Удаленный набор номера**

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

- **Транзитный вызов**

  Выберите этот режим работы для создания сервером iSeries 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.

Туннельный протокол второго уровня (L2TP): Протокол L2TP расширяет PPP путем добавления возможности организации туннелей между запрашивающим клиентом L2TP и конечной точкой целевого сервера L2TP. С помощью туннелей L2TP можно разделить точки физического подключения к сети и логического доступа к сети.

Виртуальные линии (L2TP) используются провайдерами Internet (ISP) для организации виртуальных частных сетей (VPN). Работа VPN по L2TP объясняется в разделе Настройка соединения L2TP с защитой VPN.

Ниже приведены примеры реализации туннелей L2TP:

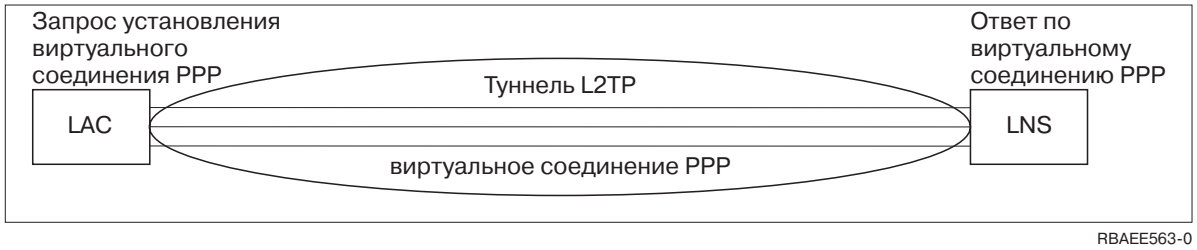

Рисунок 7. Виртуальный вызов PPP или виртуальный ответ PPP

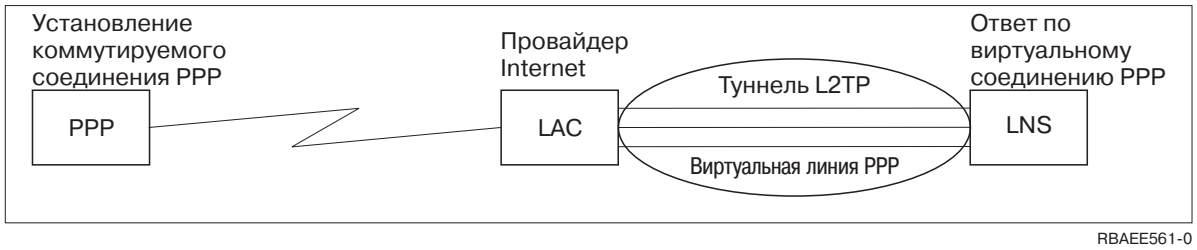

Рисунок 8. Набор номера PPP или виртуальный ответ PPP Virtual Terminator

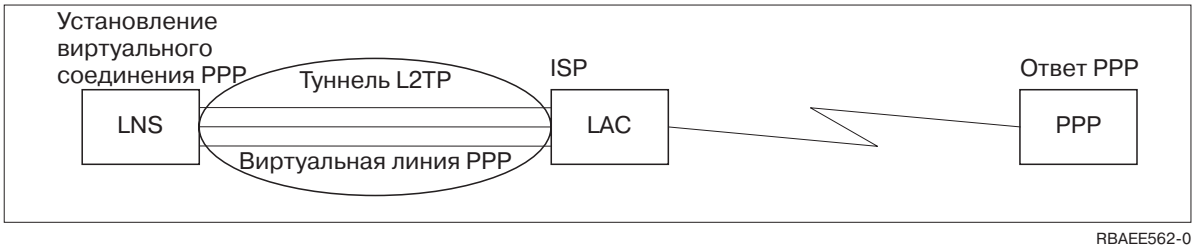

Рисунок 9. Виртуальный набор номера PPP или виртуальный ответ PPP

Линия PPPoE

Соединения PPPoE применяют виртуальные линии для отправки данных PPP через адаптер Ethernet 2838 на предоставленный провайдером Internet модем DSL, соединенный с локальной сетью на основе Ethernet. Это позволяет обеспечить высокоскоростной доступ к Internet для пользователей локальной сети с помощью сеансов PPP через сервер iSeries. После установления соединения между iSeries и провайдером Internet (ISP) пользователи локальной сети (LAN) получают доступ к ISP по соединению PPPoE iSeries.

Соединения PPPoE используются только профайлами исходящих соединений, 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.

- Отдельная линия
- Пул линий
- Линия ISDN

Отдельная линия

Выберите это значение, если соединения 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 сервера iSeries.

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 iSeries 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.

  Сервер iSeries 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.

Поддержка профайлов 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 iSeries 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, а также адаптеров 2750 и 2751, поддерживающих 8 независимых соединений ISDN по B-каналу.

Число линий из пула, используемых профайлами с поддержкой нескольких соединений, ограничено параметром Максимальное число соединений. Фактически для каждой линии пула запускается собственное задание 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 iSeries. Для выбора адреса при настройке применяется выпадающий список Локальные IP-адреса. Выбор 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 сервера iSeries отсутствует, или вы не хотите, чтобы удаленные пользователи получали доступ к локальной сети, системе iSeries 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 адрес не связан с физической сетью, он не позволяет автоматически перенаправлять данные в сетях, к которым подключена локальная система iSeries.

Для создания виртуального IP-адреса выполните следующие действия:

1. В Навигаторе выберите свой сервер 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 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 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:

В профайлах с поддержкой нескольких соединений могут применяться пулы удаленных IP-адресов. 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.

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, ISDN 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 адрес будет занят, то удаленной системе будет выделен первый доступный IP-адрес из диапазона, определяемого параметром Число адресов. Предположим, что в поле Начальный IP-адрес указано значение 10.1.1.1, а в поле Число адресов - значение 5. В этом случае пул будет состоять из следующих 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 адреса из пула уже заняты, то все последующие запросы на соединение будут отклоняться до тех пор, пока не освободится какой-нибудь адрес.
- Для того чтобы присвоить фиксированные адреса набору конкретных систем и позволить остальным системам динамически получать 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 iSeries сначала проверяет, назначен ли ему фиксированный IP-адрес. Если фиксированный адрес назначен, то он автоматически присваивается удаленной системе. В противном случае, для нее выбирается адрес из пула IP-адресов.

ISDN

Выберите это значение, если к вашей системе подключена линия ISDN.

Преимущества ISDN:

- Линии ISDN позволяют создавать быстрые соединения с низким уровнем помех.
- Сети ISDN предназначены для высокоскоростной передачи любых типов данных с единым интерфейсом.
- Коммутируемые соединения ISDN устанавливаются достаточно быстро. В среднем модемное соединение устанавливается примерно 30 секунд, в то время как для установления соединения ISDN требуется всего несколько секунд.

Настройка модема для работы с PPP

Для аналоговых соединений PPP может применяться внешний модем, внутренний модем или терминальный адаптер ISDN. Модем обеспечивает возможность аналогового соединения (по выделенной или коммутируемой линии). Описания многих модемов уже определены в системе iSeries.

Для настройки модема нужно выполнить следующие задачи:

- Настройка нового модема
- Связывание модема с описанием линии
- Задание командных строк модема

Настройка нового модема

1. В Навигаторе выберите свой сервер 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.
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.

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

1. В Навигаторе выберите свой сервер 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.

Для создания описания модема выполните следующие действия:

1. В Навигаторе откройте раздел **Сеть–> Службы удаленного доступа**.
2. Выберите **Модемы**.
3. В списке модемов щелкните правой кнопкой мыши на строке **$generic hayes** и выберите **Создать модем на основе выбранного**.
4. В окне диалога **Создать модем** введите командные строки, соответствующие модему.

Задание командных строк модема

В следующей таблице показан минимальный набор команд, поддерживаемый большинством модемов, работающих с системой iSeries. Командные строки, соответствующие вашему модему, должны быть приведены в его документации. При создании модема укажите параметры, рекомендованные его производителем.

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)	
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*, 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

1. В Навигаторе 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.
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 iSeries

   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*) позволяет 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.

Связывание модема с описанием линии

1. В Навигаторе 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 диалога свойств новой линии связи нажмите **Создать**.
4. В окне диалога 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.

В версии V5R2 профайлы исходящих соединений могут ″одалживать″ линию PPP и модем, связанные с профайлом входящих соединений, ожидающим входящего звонка. 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.

Настройка удаленного PC

Для подключения к серверу iSeries 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 на PC приведена в документации к 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 MD-5 CHAP (MS-CHAP НЕ поддерживается сервером iSeries). В некоторых версиях Windows нет встроенной поддержки MD-5 CHAP, но ее можно включить с помощью дополнительных указаний от Microsoft.
- При применении незашифрованных (или незащищенных) паролей будет автоматически использоваться протокол PAP. Это единственный незащищенный протокол, поддерживаемый сервером iSeries.
- Обычно адресация IP задается удаленной системой, в данном случае сервером iSeries. Для применения альтернативных способов адресации IP (таких как задание своих IP-адресов) необходимо убедиться в том, что сервер iSeries 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

IBM предоставляет доступ к Internet через сеть AT&T Global Network. 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 двух типов:

- **Почтовая программа**: Позволяет периодически получать почту с помощью единой учетной записи в AT&T и передавать ее в систему iSeries 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)
- 2761: 8-портовый IOA аналогового модема
- 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 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 Навигаторе выберите свой сервер 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.

Мастеры соединений

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.

Мастер универсальных соединений

Этот мастер поможет вам последовательно выполнить действия по настройке профайла соединения с IBM для электронной поддержки клиентов. Электронная поддержка клиентов обеспечивает

отслеживание конкретной среды iSeries и предоставление рекомендаций при возникновении проблем.Дополнительная информация о мастере приведена в электронной справке.

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 групповой стратегии доступа выполните следующие действия:

1. В Навигаторе выберите свой сервер 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 16 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 сервер iSeries сможет работать в качестве маршрутизатора для этого соединения. Это позволит пересылать дейтаграммы протокола IP, не предназначенные для данного сервера iSeries, 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 данного сервера iSeries.

     Пересылку IP можно запретить из соображений защиты. Провайдеры Internet, напротив, часто разрешают 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 TCP/IP.
   - 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 сервер iSeries устанавливает соединение без сжатия.
   - Применять фильтрацию IP-пакетов

     Эта опция указывает, разрешена ли фильтрация IP-пакетов. Фильтрация пакетов позволяет управлять доступом IP-пакетов в сеть. Фильтрацию IP-пакетов можно применять для защиты

системы. Она позволяет отбрасывать пакеты IP в соответствии и указанными правилами. Пакеты фильтруются в зависимости от их заголовков.

Дополнительная информация о правилах фильтрации IP-пакетов приведена в разделе IP Packet Filtering and NAT в Information Center.

Пример приведен в разделе Управление доступом пользователей к ресурсам с помощью Групповых стратегий доступа и Фильтрации IP-адресов.

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. Откройте страницу **Идентификация**.
2. Отметьте переключатель **Обязательная проверка и идентификация удаленных систем**.
3. Выберите **Локальная идентификация с помощью контрольного списка**.
4. Если в системе есть контрольный список, выберите его в выпадающем 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 диалога Добавление пользователя выполните следующие действия:
   - Выберите протокол идентификации, для которого задается имя пользователя.
   - Введите имя пользователя и пароль.

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

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

Применение правил фильтрации IP-пакетов в соединениях PPP

В разделе Правила фильтрации IP-пакетов и правила NAT справочной системы Information Center описаны способы создания правил фильтрации IP-пакетов, которые можно применять в профайлах соединений PPP. С помощью файла правил фильтрации пакетов можно ограничить доступ пользователя или группы к IP-адресам в локальной сети. Пример использования файла правил фильтрации пакетов для соединения PPP приведен в разделе Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов.

Применение правил фильтрации IP-пакетов возможно на двух уровнях:

- 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 выпадающем 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 выпадающем списке.
4. Нажмите **OK** для применения фильтра PPP.

Включение служб RADIUS и DHCP для профайлов соединений

Для включения служб RADIUS и DHCP для профайла входящих соединений PPP выполните следующие действия:

1. В Навигаторе 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 пункт **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 OK для возврата к окну Навигатора.

Пример конфигурации сервера RADIUS приведен в сценарии Идентификация коммутируемых соединений с помощью сервера RADIUS.

Глава 7. Управление PPP

Сервер iSeries поддерживает выполнение нескольких заданий управления PPP.

- Задание свойств профайлов соединений
- Монитор PPP

Задание свойств профайла соединения PPP

При создании профайла соединения в окне диалога 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 диалога **Свойства нового профайла PPP** можно воспользоваться следующими рекомендациями. Значения свойств зависят от среды и типа настраиваемого соединения. Все опции окна диалога описаны в электронной справке Навигатора. Дополнительная информация приведена в примерах PPP и процедурах.

Монитор PPP

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

О заданиях соединения PPP:

- Управлять отдельными заданиями соединений PPP можно с помощью двух контрольных заданий PPP. Эти задания работают в подсистеме QSYSWRK:
  - QTPPPCTL - Основное управляющее задание PPP. Это задание управляет всеми заданиями соединений PPP.
  - QTPPPL2TP - Сервер L2TP. Это задание управляет организацией туннелей L2TP и работает только при запущенном профайле L2TP.
- Задания соединений PPP работают только с пользовательским профайлом QTCP и применяются для обработки отдельных соединений PPP. По умолчанию эти задания работают в подсистеме QUSRWRK, но их можно настроить для работы в других подсистемах. В системе используются два разных типа заданий для обработки соединений PPP:
  - QTPPPSSN - Это задание применяется для обработки соединений PPP без поддержки L2TP:
  - QTPPPL2SSN - Задания, обрабатывающие данные виртуального PPP после того, как задание QTPPPL2TP успешно установит соединение L2TP.
- 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*nn* соответствуют входящим звонкам, где *nn* - число от 1 до 99.

Работа с профайлами соединений:

1. В Навигаторе выберите свой сервер 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:
   - **Задания** - будет показан протокол задания QTPPP*xxx*.
   - **Соединения** - будет показано окно диалога 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 задания можно просмотреть либо вывод задания, либо подробную информацию о соединении.

- **Свойства** - будут показаны параметры соединения.

Просмотр информации о соединении:

1. В Навигаторе выберите свой сервер 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, локальный и удаленный IP-адреса и имя задания PPP, будет показана в зависимости от состояния каждого задания PPP.
3. Для просмотра вывода или подробной информации о соединении щелкните правой кнопкой мыши на соединении.
4. Для просмотра вывода задания нажмите **Задания**. В протоколе задания щелкните правой кнопкой мыши на имени задания и выберите **Вывод на принтер**. Затем можно просмотреть журналы и протоколы задания (для завершенных заданий) сеансов соединений.
5. Для просмотра подробной информации о соединении нажмите **Сведения**. Эту информацию можно просмотреть только для активных соединений. Окно диалога Сведения позволяет просмотреть дополнительную информацию о конкретном соединении.

Работа с выводом PPP с сервера iSeries:

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

- 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 диалога Соединения.

Основное состояние	Описание
Ожидание запросов на создание соединения	Профайл входящих соединений готов к созданию соединения
Ожидание входящего звонка	Сервер готов к установлению соединения
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

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

Глава 8. Устранение неполадок PPP

Свежая информация о временных исправлениях программ (PTF) и устранении неполадок приведена на домашней странице TCP/IP сервера iSeries . В разделе под этой ссылкой приведена информация, дополняющая и заменяющая информацию этого раздела.

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

1. Обязательная информация:
   - Тип удаленного хоста, его операционная система и версия системы
   - Версия операционной системы локального хоста сервера iSeries
   - Протокол задания сеанса, в котором произошел сбой, и файл диалога соединения

     В OS/400 выпуска V5R1 протоколы заданий и файлы диалога соединений сохраняются в библиотеке OUTQ под именем профайла.
   - Сценарий соединения (если применяется)
   - 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

В книге ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) дано расширенное описание перечисленных ниже неполадок PPP. В ней также приведена подробная информация по их устранению.

Неполадка	Способ устранения
Аппаратная конфигурация модема Неверная конфигурация переключателей и других аппаратных настроек	Убедитесь, что модем настроен для работы в правильном режиме обработки кадров. 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 Навигатора.	Создайте новое определение 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.

Неполадка	Способ устранения
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.
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.

Глава 9. Дополнительная информация о PPP

Прочие источники информации по PPP:

- Для перехода к последним версиям временных исправлений программ (PTF) и свежей информации о настройке PPP и L2TP выберите ссылку PPP на домашней странице TCP/IP сервера iSeries  . В разделе под этой ссылкой приведена наиболее свежая информация, дополняющая и заменяющая информацию в разделе **Службы удаленного доступа: Соединения PPP**.
- В книге ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  приведена обширная информация о службах и приложениях TCP/IP.

IBM Confidential
Напечатано в Дании