Технология удаленного доступа: Обзоры и объяснения

Содержание

Введение

Эта глава представляет и объясняет некоторые технологии, используемые в коммутируемых сетях. Вы найдете советы конфигурации и интерпретации некоторых **команд показа**, которые полезны для проверки нормальной работы сети. Процедуры устранения проблем выходят за рамки этого документа и могут быть найдены в документе, названном*, Устранив неполадки Коммутируемого доступа*.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Функционирования модема

Этот раздел объясняет проблемы, отнесенные в частности к настройке, проверке и использованию модемов с маршрутизаторами Cisco.

Использование команды функций автонастройки модема

При использовании операционной системы межсетевого взаимодействия Cisco IOS (Cisco IOS) Выпуск 11.1 или позже можно настроить маршрутизатор Cisco, чтобы связаться с и настроить модем автоматически.

Используйте следующую процедуру для настройки маршрутизатора Cisco, чтобы автоматически попытаться обнаружить, какой модем связан с линией, и затем настраивать модем:

1. Для обнаружения типа модема, подключенного к маршрутизатору, используйте команду конфигурации с командной строки **modem autoconfigure discovery**.
2. Когда модем будет успешно обнаружен, настройте модем автоматически с помощью команды *modem autoconfigure type modem-name line configuration*.

Если вы хотите отобразить список модемов, для которых маршрутизатор имеет записи, используйте *название модема* **show modemcap**. Если вы хотите изменить значение модема, которое было возвращено из **команды show modemcap**, используйте команду конфигурации с командной строки *значения атрибута имени модема* **modemcap edit**.

Для полной информации на использовании этих команд обратитесь к *Набираемому Справочнику по командам Решений для Руководства по конфигурации и Набора Решений для документации по Cisco IOS*.

Примечание: *Не* вводите **&W** в запись "Modemcap", которая используется для автоматического конфигурирования. Это заставляет NVRAM быть переписанным каждый

раз, когда функции автонастройки модема выполнены и уничтожат модем.

Установка обратного сеанса Telnet с модемом

Для диагностических назначений, или первоначально настраивать модем при выполнении Cisco IOS Release 11.0 или ранее необходимо установить обратное telnet-соединение для настройки модема для передачи с устройством Cisco. Пока вы блокируете скорость модема стороны терминального оборудования пользователя (DTE), модем будет всегда связываться с сервером доступа или маршрутизатором в нужной скорости. См. Таблицу 16-5 для получения информации о блокировке скорости модема. Убедитесь, что скорость устройства Cisco настроена прежде, чем дать команды к модему через обратное telnet-соединение. Снова, обратитесь к Таблице 16-5 для получения информации о настройке скорости сервера доступа или маршрутизатора.

Для настройки модема для обратного telnet-соединения используйте **команду настройки из командной строки transport input telnet**. Устанавливать групповой номер (в этом случае, на порту 1), вводят **команду rotary 1** конфигурации с командной строки. Размещение этих команд под конфигурацией с командной строки заставляет IOS выделять слушателей IP для входящих соединений в диапазонах портов начиная со следующих оснований:

2000	Telnet протокол
3000	Протокол Telnet с ротацией
4000	Протокол Raw TCP
5000	Протокол Raw TCP с ротацией
6000	Протокол Telnet, бинарный режим
7000	Протокол Telnet, бинарный режим с ротацией
9000	Протокол xremote
10000	Протокол xremote с ротацией

Для инициирования обратного telnet-соединения к модему выполните следующие шаги:

1. От вашего терминала используйте **telnet ip-address 20yy** команды, где *IP-адресом* является IP-адрес любого активного, связанный интерфейс на устройстве Cisco, и yy является номером строки, с которым связан модем.Например, следующая команда подключила бы вас со вспомогательным портом на маршрутизаторе Cisco 2501 с IP-адресом 192.169.53.52: **telnet 192.169.53.52 2001**. Обычно Команда telnet этого вида может быть выполнена отовсюду в сети, если это может **пропинговать** рассматриваемый IP-адрес.**Примечание:** На большинстве маршрутизаторов Cisco порт 01 является вспомогательным портом. На Сервере доступа Cisco вспомогательным портом является последний TTY +1. Как пример, вспомогательный порт на 2511 является портом 17 (16 портов TTY + 1). Всегда используйте команду exec **выставочного подвида** для обнаружения номера вспомогательного порта - особенно на серии 2600 и 3600, которые используют номера портов состоящие из нескольких несмежных участков для размещения переменных асинхронных размеров модуля.
2. Если соединению отказывают, оно могло бы указать, что существует или никакой слушатель в указанном адресе и порту, или что кто-то уже связан с тем портом. Проверьте адрес соединения и номер порта. Кроме того, удостоверьтесь **команда modem inout** или **modem DTR-active**, а также **transport input all**, появитесь под

конфигурацией с командной строки для достигаемых линий.При использовании функции чередования удостоверьтесь*, что ротация* команды *n* также появляется в конфигурации с командной строки, где n является количеством группового номера. Проверять, связан ли кто-то уже, telnet к маршрутизатору и использует *команду show line n*. Ищите звездочку, чтобы указать, что используется линия. Удостоверьтесь, что CTS высок, и DSR не. Используйте *команду clear line n* для разъединения текущего сеанса на номере порта n. Если соединению все еще отказывают, модем мог бы утверждать Обнаружение несущей (CD) все время. Разъедините модем от линии, установите обратное telnet-соединение, и затем подключите модем.

3. После успешного создания Telnet - подключения введите AT и быть уверенными ответы модема с OK.
4. Если модем не является быстро реагирующим, обратитесь к следующей таблице.

Таблица 16-1 ниже выделяет возможные причины симптомов проблемы модема к подключению маршрутизатора и описывает решения тех проблем.

Таблица 16-1: никакое подключение между модемом и маршрутизатором

Возможные причины	**Предлагаемые действия**
Управление по модему не включено на сервере доступа или маршрутизаторе	1. **Используйте show line exec command на сервере доступа или маршрутизаторе.** Выходные данные для вспомогательного порта должны показать **InOut** или **RIisCD** в Столбце модема. Это указывает, что управление по модему включено на линии сервера доступа или маршрутизатора. Для пояснения **выходных данных show line** обратитесь к "Использованию Команд отладки" в главе 15. 2. Настройте линию для управления по модему с помощью команды конфигурации с командной строки **ввод-вывода модема**. Управление по модему теперь включено на сервере доступа. Пример: Следующий пример иллюстрирует, как настроить линию для обоих входящих и исходящих звонков: `line 5` `modem inout` **Примечание:** Обязательно используйте **команду modem inout**, а не **команду modem dialin**, в то время как подключение модема рассматриваемо. Последняя команда позволяет линии принимать входящие вызовы только. Исходящим вызовам

	откажут, и будет невозможно установить сеанс Telnet с модемом для настройки его. Если вы хотите использовать **команду modem dialin**, сделайте так только после того, как вы уверены, что модем функционирует правильно.
Модем мог быть неправильно сконфигурирован или иметь зависание сеанса.	Введите **AT&FE1Q0**, чтобы возвратить его к заводским настройкам и удостовериться, что модем собирается повторить символы и возвратить выходные данные. Модем может иметь зависание сеанса. Используйте **"^U"** для очистки линии и **"^Q"** для открытия управления потоками (XON). Проверьте параметры контроля четности.
Неверная разводка кабелей	1. Проверьте кабельное подключение между модемом и сервером доступа или маршрутизатором. Подтвердите, что модем связан со вспомогательным портом на сервере доступа или маршрутизаторе с прокрученным кабелем RJ-45 и адаптером DB-25 MMOD. Эта конфигурация разводки кабелей рекомендуется и поддерживается Cisco для портов RJ-45. (Эти разъёмы, как правило, маркируются "Модем".) 2. Используйте команду exec **выставочного подвида**, чтобы проверить, что кабельное подключение корректно. Посмотрите, что пояснение выходных данных **команды show line** в разделе назвало "Использование Команд отладки" в главе 15.
Неполадка в оборудовании	1. Проверьте использование правильной разводки кабелей и что все соединения хороши. 2. Проверьте все аппаратные средства для повреждения, включая кабельное подключение (поврежденных проводок), адаптеров (свободные контакты), порты сервера доступа и модем. 3. См. Главу 3, "Устранив неполадки Аппаратных средств и Проблем загрузки", для получения

	дополнительной информации об устранении проблем оборудования.

Использование групповых номеров

Для некоторых приложений модемы на данном маршрутизаторе должны быть разделены группой пользователей. Служебная программа Cisco dialout utility является примером этого типа приложения. В основном пользователи соединяются с одним портом, который подключает их с доступным модемом. Для добавления асинхронной линии к групповому номеру просто введите **ротацию** *n*, где *n* является количеством группового номера в конфигурации для асинхронной линии. См. пример ниже.

```
line 1 16
 modem InOut
 transport input all
 rotary 1
 speed 115200
 flowcontrol hardware
```

Вышеупомянутая конфигурация с командной строки позволила бы пользователям соединяться с групповым номером путем ввода **telnet 192.169.53.52 3001** для обычного telnet. Альтернативы включают порты 5001 для Необработанного TCP, 7001 для двоичного Telnet (который служебная программа Cisco dialout utility использует), и 10001 для подключений Xremote.

Примечание: Чтобы проверить конфигурацию служебной программы Cisco dialout utility, дважды щелкают по значку утилиты установления внешнего телефонного соединения в правом нижнем углу экрана и нажать More> кнопка. Затем, нажмите Configure Ports> кнопка. Удостоверьтесь, что порт находится в этих 7000 диапазонов при использовании групповых номеров и этих 6000 диапазонов, если Утилита установления внешнего телефонного соединения предназначается для отдельного модема. Необходимо также включить модем, входящий в систему ПК. Это сделано путем выбора следующей последовательности: **запустите-> Панель управления-> модемы->** (выберите свой модем исходящих звонков удаленного доступа Cisco)-> **Свойства-> Соединение-> Усовершенствованный**...-> **Запись файл журнала**.

Интерпретация выходных данных Show Line

Выходные данные от команды exec *line-number* **выставочного подвида** полезны при устранении проблем подсоединения модема к серверу доступа или маршрутизатору. Ниже выходные данные от **команды show line**.

```
as5200-1#show line 1 Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int 1 TTY
115200/115200- - - - - 0 0 0/0 - Line 1, Location: "", Type: "" Length: 24 lines, Width: 80
columns Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits Status: No Exit
Banner Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out Modem state: Hanging up
modem(slot/port)=1/0, state=IDLE dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED Group
codes: 0 Modem hardware state: CTS noDSR noDTR RTS Special Chars: Escape Hold Stop Start
Disconnect Activation ^^x none - - none Timeouts: Idle EXEC Idle Session Modem Answer Session
Dispatch 00:10:00 never none not set Idle Session Disconnect Warning never Login-sequence User
Response 00:00:30 Autoselect Initial Wait not set Modem type is unknown. Session limit is not
set. Time since activation: never Editing is enabled. History is enabled, history size is 10.
DNS resolution in show commands is enabled Full user help is disabled Allowed transports are lat
pad telnet rlogin udptn v120 lapb-ta. Preferred is l at pad telnet rlogin udptn v120 lapb-ta. No
output characters are padded No special data dispatching characters as5200-1#
```

Когда неполадки подключения происходят, важные выходные данные появляются в Состоянии модема и Полях состояния оборудования модема.

Примечание: Поле состояния оборудования модема не появляется в **выходных данных show line** для каждой платформы. В определенных случаях индикации для состояний сигнала покажут в поле Состояния модема вместо этого.

Таблица 16-2 показывает типичные строки Состояния модема и Состояния оборудования модема от выходных данных **команды show line**. Это также объясняет значение каждого состояния.

Таблица 16-2: модем и состояния оборудования модема в выходных данных Show Line

Состояние модема	Состояние оборудования модема	Значение
Простаивающий	RTS DTR noDSR CTS	Это надлежащие состояния модема для соединений между сервером доступа или маршрутизатором и модемом (когда нет никакого входящего вызова). Выходные данные любого другого вида обычно указывают на проблему.
ГОТОВО	-	Если состояние модема Готово вместо Айдла, рассмотрите придерживающееся: 1. Управление по модему не настроено на сервере доступа или маршрутизаторе. Настройте сервер доступа или маршрутизатор с командой конфигурации с командной строки **ввод-вывода модема**. 2. Сеанс существует на линии. Используйте команду exec **show users** и используйте **команду clear line privileged exec** для остановки сеанса при желании. 3. DSR высок. Существует две возможных причины для этого: Проблемы с кабельным соединением. Если ваш разъём использует контакт 6 DB-25 и не имеет никакого контакта 8, необходимо

		переместить контакт от 6 до 8 или получить соответствующий разъём.Модем, настроенный для DCD, всегда высок. Модем должен быть реконфигурирован для имения высокого значения DCD только один CD (1). Это обычно делается с **&C1** командами модема, но проверьте свою документацию по модему для точного синтаксиса для вашего модема. Если ваше программное обеспечение не поддерживает управление по модему, необходимо настроить канал сервера доступа, с которым модем связан с командой конфигурации с командной строки **no exec**. Очистите линию с **командой clear line privileged exec**, инициируйте обратное telnet-соединение с модемом и реконфигурируйте модем так, чтобы DCD был высоко только на CD. Закончите сеанс Telnet путем ввода **разъединения** и реконфигурируйте канал сервера доступа с командой конфигурации с командной строки exec.
ГОТОВО	noCTS noDSR DTR RTS (2)	Строка noCTS появляется в Поле состояния оборудования модема по одной из следующих четырех причин: 1. Модем выключен. 2. Модем должным образом не связан с сервером доступа. Проверьте телеграфирующие соединения от модема до сервера доступа. 3. Неверная разводка кабелей (или витой mdce, или прямой MDTE, но без перемещенных контактов). Рекомендуемая конфигурация каблирования

		дана ранее в этой таблице. 4. Модем не настроен для аппаратного управления потоками. Не используйте команду конфигурации с командной строки **аппаратного обеспечения "по управлению потоком данных"** для отключения аппаратного управления потоками на сервере доступа. Затем включите аппаратное управление потоками на модеме через обратное telnet-соединение. (Консультируйтесь со своей документацией по модему и посмотрите, что раздел "Устанавливает Обратное telnet-соединение к Модему" ранее в этой главе.) Реактивируют аппаратное управление потоками на сервере доступа с командой конфигурации с командной строки **аппаратного обеспечения "по управлению потоком данных"**.
ГОТОВО	RTS DTR DSR CTS (2)	Строка DSR (вместо строки noDSR) появляется в Поле состояния оборудования модема по одной из следующих причин: 1. Неверная разводка кабелей (или витой mdce, или прямой MDTE, но без перемещенных контактов). Рекомендуемая конфигурация каблирования дана ранее в этой таблице. 2. Модем настроен для DCD всегда высоко. Реконфигурируйте модем так, чтобы DCD был только высок на CD. Это обычно делается с **&C1** командами модема, но проверьте свою документацию по модему для точного синтаксиса для вашего

		модема. Настройте канал сервера доступа, с которым модем связан с командой конфигурации с командной строки **no exec**. Очистите линию с **командой clear line privileged exec**, инициируйте обратное telnet-соединение с модемом и реконфигурируйте модем так, чтобы DCD был высоко только на CD. Закончите сеанс Telnet путем ввода **разъединения**. Реконфигурируйте канал сервера доступа с командой конфигурации с командной строки exec.
ГОТОВО	CTS* DSR* RTS DTR (2)	Если эта строка появляется в Поле состояния оборудования модема, управление по модему, вероятно, не включено на сервере доступа. Используйте команду конфигурации с командной строки **ввод-вывода модема** для включения управления по модему на линии. Дополнительные сведения о настройке управления по модему на сервере доступа или линии маршрутизатора предоставлены ранее в этой таблице.

(1) CD = определение несущей

(2) * рядом с сигналом указывает на одну из двух вещей: сигнал изменился в течение прошлых нескольких секунд, или сигнал не используется выбранным методом управления по модему.

Сбор сведений о производительности модема

Этот раздел объясняет методы для сбора производительности данных на цифровых модемах MICA, найденных в семействе Cisco AS5x00 серверов доступа. Производительность данных может использоваться для анализа тенденции изменения и полезна в устранении проблем проблем производительности, с которыми можно было бы встретиться. При рассмотрении номеров, представленных ниже, примите во внимание, что совершенство не возможно в реальных условиях. Возможная доля успешных попыток модемного вызова (CSR) является функцией качества каналов, базы пользователей клиентского модема и набора используемых модуляций. Типичный процентный показатель CSR для вызовов V.34 составляет 95%. Вызовы V.90, как могут ожидать, подключат успешно 92% времени. Преждевременные отбрасывания, вероятно, произойдут 10% времени.

Используйте следующие команды для получения полного представления поведения модема на сервере доступа:

- **show modem**
- **show modem summary**
- **show modem connect-speeds**
- **show modem call-stats**

Следующая информация полезна при устранении проблем соединения отдельного модема или сборе данных для анализа тенденции изменения:

- debug modem csm
- modem call-record terse
- show modem op (MICA) / AT@E1 (Microcom), в то время как связано
- show modem log для сеанса интереса после разъединения
- ANI (номер абонента)
- Время дня
- Аппаратные средства клиентского модема / редакция микропрограммного обеспечения
- Содержательные данные от клиента (после того, как разъединение) - ATI6, ATI11, AT&V, AT&V1, и так далее
- Аудио запись (файл .wav) пробного подключения пытается от клиентского модема

В следующих разделах команды будут объяснены далее, и будут обсуждены некоторые общие тенденции.

Show Modem / Show Modem Summary

Команда show modem высказывает мнение отдельных модемов. От этих номеров может быть просмотрено состояние отдельных модемов.

```
router# show modem Codes: * - Modem has an active call C - Call in setup T - Back-to-Back test in progress R - Modem is being Reset p - Download request is pending and modem cannot be used for taking calls D - Download in progress B - Modem is marked bad and cannot be used for taking calls b - Modem is either busied out or shut-down d - DSP software download is required for achieving K56flex connections ! - Upgrade request is pending Inc calls Out calls Busied Failed No Succ Mdm Usage Succ Fail Succ Fail Out Dial Answer Pct. * 1/0 17% 74 3 0 0 0 0 0 96% * 1/1 15% 80 4 0 0 0 1 1 95% * 1/2 15% 82 0 0 0 0 0 0 100% 1/3 21% 62 1 0 0 0 0 0 98% 1/4 21% 49 5 0 0 0 0 0 90% * 1/5 18% 65 3 0 0 0 0 0 95%
```

Для наблюдения номеров агрегации для всех модемов на маршрутизаторе используйте **команду show modem summary**.

```
router#show modem summary Incoming calls Outgoing calls Busied Failed No Succ Usage Succ Fail Avail Succ Fail Avail Out Dial Ans Pct. 0% 6297 185 64 0 0 0 0 0 0 97%
```

Таблица 16-3: Поля show modem

Поля	Описания
Входящие и исходящие звонки	Вызывает набор номера в и из модема. • Использование - Процент от времени работы без сбоев всей системы, что используются все модемы. • Succ - Общие количества вызовов успешно соединились. • Сбой - Общие количества вызовов,

	которые успешно не соединились. • Польза - Общие модемы, доступные для использования в системе.
Занятый	Общее число времен модемы было взято вне обслуживания с командой **modem busy** или **командой modem shutdown**.
Отказавший набор	Общее число попыток, модемы не зависали или было нет тонового соединения.
No Ans	Общее число оповещения о вызове звонком времен было обнаружено, но звонки не ответил модем.
Процент Succ.	Процент успешного подключения от общих доступных модемов.

Выходные данные Show Modem Call-Stats

```
compress  retrain lostCarr  rmtLink  trainup hostDrop wdogTimr inacTout
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %
 Total    9       41      271     3277        7     2114        0        0
```

Таблица 16-4: Поля show modem call-stats

rmt Link	Этот показ, что исправление ошибок было в действительности, и вызов, зависся системой клиента, подключенной к удаленному модему.
hostDrop	Это показывает, что вызов зависся системой хоста IOS. Некоторые обычные причины включают: время простоя, канал очищается от телефонной компании или LCP PPP termreq от клиента. Лучший способ определить причину для зависания при помощи краткого modem call-record или учет AAA.

Другие причины разъединения должны составить в целом меньше чем 10% общего количества.

Выходные данные Show Modem Connect-Speeds

```
router>show modem connect 33600 0
 Mdm   26400  28000  28800  29333  30667  31200  32000  33333  33600 TotCnt
Tot      614      0   1053      0      0   1682      0      0    822   6304

router>show modem connect 56000 0
 Mdm   48000  49333  50000  50666  52000  53333  54000  54666  56000 TotCnt
Tot      178    308     68     97     86     16      0      0      0   6304
```

Ожидайте видеть распределение скоростей V.34. Должен быть пик в 26.4, если сигнализация по выделенному каналу (CAS) использования T1s. Для ISDN (PRI) T1s пик должен быть в 31.2. Кроме того, ищите некоторых K56Flex, скорости V.90. Если нет никаких соединений V.90 может быть проблема топологии сети.

Понимание Modem Call-Record краткая (11.3AA/12.0T) команда

Вместо команды exec, это - команда настройки, размещенная в уровень системы рассматриваемого сервера доступа. Когда пользователь разъединяет, сообщение, подобное следующим показам:

```
*May 31 18:11:09.558: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=2/0/18,
slot/port=1/29, call_id=378, userid=cisco, ip=0.0.0.0, calling=5205554099,
called=4085553932, std=V.90, prot=LAP-M, comp=V.42bis both,
init-rx/tx b-rate=26400/41333, finl-rx/tx brate=28800/41333, rbs=0, d-pad=6.0 dB,
retr=1, sq=4, snr=29, rx/tx chars=93501/94046, bad=5, rx/tx ec=1612/732, bad=0,
time=337, finl-state=Steady, disc(radius)=Lost Carrier/Lost Carrier,
disc(modem)=A220 Rx (line to host) data flushing - not OK/EC condition - locally
detected/received
DISC frame -- normal LAPM termination
```

Команда Show Modem Operational-Status

Эксплуатационное состояние модема exec command show показывает ток (или новый) параметры, имеющие отношение к соединению модема.

Запись в документации для этой команды найдена в *Набираемом Справочнике по командам Решений для Cisco IOS Release 12.0*. **show modem operational-status** только для Модемов MICA. Аналогичная команда для Модемов microcom является **modem at-mode / AT@E1**. Используйте **modem at-mode <слот> /** команда **<port>** для соединения с модемом, затем выполните **команду AT@E1**. Подробная документация для **команды modem at-mode** может быть найдена в *Руководстве по конфигурации программного обеспечения Cisco AS5300*, и документация для **команды AT@E1** находится в *наборе AT-команд и Сводке реестра для Справочника по командам Модулей Модема microcom*.

Используйте следующие шаги для определения, на каких модемах пользователь входит:

1. Выполните **команду show user** и ищите TTY, с которым они связаны.
2. Используйте **команду show line** и ищите номера слота/порта модема.

Сбор данных о производительности на стороне клиента

Для анализа тенденции изменения очень важно собрать данные о производительности на стороне клиента. Всегда пытайтесь получить следующую информацию:

- модель/версия микропрограммы оборудования клиента (достижимый с **командой ATI3I7** на модеме клиента)
- сообщаемые клиентами причины разъединения (используют **ATI6** или **AT&V1**),

Другая доступная информация на клиентской стороне включает modemlog.txt и ppplog.txt ПК. Необходимо в частности настроить ПК для генерации этих файлов.

Проанализируйте производительность данных

Как только вы собрали и поняли производительность данных для своей модемной системы, необходимо посмотреть на любые остающиеся образцы и компоненты, которым, возможно, понадобится улучшение.

Проблемы с модемами индивидуального сервера

Используйте **show modem** или **show modem call-stats**, чтобы определить любые модемы с аномально высокими скоростями сбоя пробного включения или плохо разъединить скорости (MICA). Если соседние пары модемов имеют проблемы, проблема вероятна "зависнувший"/простой DSP. Используйте **copy flash modem** для HMM, на который влияют, для восстановления. Удостоверьтесь, что модемы выполняют последнюю версию микропрограммного обеспечения порта. Чтобы проверить, что все модемы правильно настроены, используйте **mica/microcom_server типа автоматического конфигурирования configuration command modem** в конфигурации с командной строки. Для проверки модемы автоматически сконфигурированы каждый раз, когда вызов зависается, используйте **debug confmodem** команды exec. Для решения проблемы модемов, которые плохо неправильно сконфигурированы, вы, возможно, должны установить обратное telnet-соединение.

Проблемы с определенными ds0

Проблемы DS0 редки, но возможны. Для определения местоположения неправильно функционирующих Ds0 используйте **show controller t1 call-counters** команды и ищите любые Ds0 с аномально высоким TotalCalls и неправильно низким TotalDuration. Для предназначения для подозреваемых Ds0 вам, возможно, понадобятся к занятому другие Ds0 с **dsl сервиса configuration command ISDN, busyout ds0** под последовательным интерфейсом для T1. Выходные данные от **show controller t1 call-counters** похожи на это:

```
TimeSlot   Type   TotalCalls   TotalDuration
    1       pri         873       1w6d
    2       pri         753       2w2d
    3       pri         4444      00:05:22
```

Очевидно, временной интервал 3 является подозрительным каналом в этом случае.

Дополнительные общие тенденции

Ниже несколько более общих тенденций, замеченных Центром технической поддержки Cisco.

1. Плохие пути каналаЕсли у вас есть следующие проблемы, вы могли бы получать плохие пути канала через открытую коммутируемую телефонную сеть (PSTN):междугородние вызовы имеют проблемы, но локальный не делают (или наоборот)заходит в определенное время суток, имеют проблемывызовы от определенных удаленных обменов имеют проблемы
2. Проблемы с междугородними вызовамиЕсли ваша услуга дальней связи не функционирует должным образом или вообще (но локальный сервис прекрасен):Убедитесь, что цифровой канал соединяется в цифровой коммутатор, не банк каналов.Дайте телефонным компаниям команду исследовать пути канала, используемые на большое расстояние.
3. Проблемы с вызовами от определенных областей вызова.Если вызовы от определенных географических областей/обменов имеют тенденцию иметь проблемы, необходимо получить топологию сети из телефонной компании.Если множественные преобразования аналогового сигнала в цифровой будут требоваться, то подключения модема V.90/K56flex не будут возможны, и V.34 может быть несколько ухудшен. Преобразования аналогового сигнала в цифровой требуются в областях, которые подаются неинтегрированными цифровыми коммутаторами или аналоговыми коммутаторами.

Операции ISDN

ISDN обращается к ряду цифровых сервисов, которые доступны конечным пользователям. ISDN включает оцифровку телефонной сети так, чтобы голос, данные, текст, графика, музыка, видео и другой исходный материал могли быть предоставлены конечным пользователям от одиночного, терминала конечного пользователя по проводному соединению существующего телефона. Сторонники ISDN воображают всемирную сеть во многом как существующая телефонная сеть, но с цифровой передачей и множеством новых сервисов.

ISDN является усилием стандартизировать абонентские сервисы, пользователя/сетевые интерфейсы, и сеть и возможности объединенной сети. Стандартизация абонентских сервисов пытается гарантировать уровень международной совместимости. Стандартизация пользователя/сетевого интерфейса стимулирует разработку и маркетинг этих интерфейсов сторонними изготовителями. Сеть Standardizing и возможности объединенной сети помогают достигать цели возможности подключения в любой точке мира путем обеспечения, что сети ISDN легко связываются друг с другом.

Приложения ISDN включают высокоскоростные приложения образа (такие как факсимиле IV Группы), дополнительные телефонные линии в домах для обслуживания работающей дистанционно отрасли, высокоскоростной передачи файла и видеоконференцсвязи. Голос, конечно, isl также широко используемое приложение для ISDN.

Рынок внутреннего доступа делится между другими технологиями. В областях, где более новый меньше дорогостоящих технологий, таких как DSL и Кабель становится доступным, внутренний рынок переезжает от ISDN. Компании, однако, продолжают использовать ISDN в форме T1/E1 PRI, чтобы нести большие количества данных или предоставить доступ входящего вызова v.90.

Компоненты ISDN

Компоненты ISDN включают терминалы, терминальные адаптеры (TA), сетевые оконечные устройства, оконечная аппаратура линии и оборудование завершения обмена. Терминалы ISDN прибывают в два типа. Специализированные Терминалы ISDN упоминаются как тип терминального оборудования 1 (TE1). Терминалы НЕ ISDN, такие как DTE, которые предшествуют Стандартам ISDN, упоминаются как тип терминального оборудования 2 (TE2). TE1 соединяются с сетью ISDN через четырехпроводное цифровое соединение витой пары. TE2 соединяются с сетью ISDN через терминальный адаптер. ISDN TA может или быть отдельным устройством или платой в TE2. Если TE2 внедрен как отдельное устройство, он соединяется с TA через стандартный интерфейс физического уровня. Примеры включают EIA/TIA-232-C (раньше RS-232-C), V.24 и V.35.

Вне TE1 и устройств TE2, следующая точка подключения в сети ISDN является типом оконечного устройства сети 1 (NT1) или тип оконечного устройства сети 2 (NT2) устройство. Это сетевые оконечные устройства, которые подключают четырехпроводного абонента, соединяющего проводом с обычной двухпроводной абонентской линией. В Северной Америке NT1 является устройством Customer Premises Equipment (CPE). В большинстве других частей мира NT1 является частью сети, предоставленной носителем. NT2 является более сложным устройством, как правило, найденным в цифровых учрежденческих телефонных станциях с выходом в город (PBXs), который выполняет Уровень 2 и 3 функции протокола и сервисы концентрации. Устройство NT1/2 также существует; это - одиночное устройство, которое комбинирует функции NT1 и NT2.

Много контрольных точек заданы в ISDN. Эти контрольные точки определяют логические интерфейсы между функциональными группировками, такими как TA и NT1. Контрольные точки ISDN включают придерживающееся:

- Контрольная точка R-The между отличным от ISDN оборудование и TA
- Контрольная точка S-The между терминалами пользователя и NT2
- Контрольная точка Tthe между NT1 и устройствами NT2
- Контрольная точка U-The между устройствами NT1 и оконечной аппаратурой линии в коммуникационной сети. Контрольная точка U релевантна только в Северной Америке, где функция NT1 не предоставлена коммуникационной сетью

Ниже приводится пример конфигурации ISDN. Эта выборка показывает три устройства, подключенные коммутатору ISDN в центральной АТС. Два из этих устройств СОВМЕСТИМЫ С ISDN, таким образом, они могут быть подключены через контрольную точку S к устройствам NT2. Третье устройство (стандартный, телефон не ISDN) подключает через контрольную точку R к TA. Любое из этих устройств могло также подключить к устройству NT1/2, которое заменит и NT1 и NT2. И, невзирая на то, что их не показывают, подобные пользовательские станции присоединены к крайнему справа коммутатору ISDN.

Пример конфигурации ISDN

```
2503B#show running-config Building configuration... Current configuration: ! version 11.1
service timestamps debug datetime msec service udp-small-servers service tcp-small-servers !
hostname 2503B ! ! username 2503A password ip subnet-zero isdn switch-type basic-5ess !
interface Ethernet0 ip address 172.16.141.11 255.255.255.192 ! interface Serial0 no ip address
shutdown ! interface Serial1 no ip address shutdown ! interface BRI0 description phone#5553754
ip address 172.16.20.2 255.255.255.0 encapsulation ppp dialer idle-timeout 300 dialer map ip
172.16.20.1 name 2503A broadcast 5553759 dialer-group 1 ppp authentication chap ! no ip
classless ! dialer-list 1 protocol ip permit ! line con 0 line aux 0 line vty 0 4 ! end 2503B#
```

Сервисы ISDN

Сервис Интерфейса (BRI) ISDN предлагает два канала B и один канал D (2B+D). Сервис B-канала BRI работает в 64 кбит/с и предназначается для переноса пользовательских данных; сервис Канала D BRI работает в 16 кбит/с и предназначается для переноса контроля и сигнальной информации, невзирая на то, что это может поддержать передачу пользовательских данных при определенных обстоятельствах. Протокол Сигнализации по каналу D включает Уровни 1 через 3 из Эталонной модели OSI. BRI также обеспечивает управление формированием кадров и другие издержки, принося ее общую скорость передачи к 192 кбит/с. Спецификацией физического уровня BRI является Отдел стандартизации электросвязи международного союза электросвязи (ITU-T; раньше Консультативный комитет по международной телеграфной и телефонной связи [CCITT]) Я 430.

Интерфейс первичного уровня ISDN (PRI), который сервис предлагает 23 каналам B и одному каналу D в Северной Америке и Японии, приводя к общей скорости передачи 1.544 Мбит/с (канал D PRI достигает 64 кбит/с). PRI ISDN в Европе, Австралии и других частях мира предоставляет 30 B плюс один канал D на 64 кбит/с и скорость общей скорости интерфейса 2.048 Мбит/с. Спецификация физического уровня PRI является ITU-T Я 431.

Уровень 1

Физический уровень ISDN (Уровень 1), форматы фрейма отличаются в зависимости от того, является ли кадр исходящим (от терминала до сети) или входящим (с сети на терминал).

Оба интерфейса физического уровня показывают на рисунке 16-1.

Рисунок 16-1: форматы фрейма физического уровня ISDN

Кадры 48 битов длиной, которых 36 битов представляют данные. Биты фрейма физического уровня ISDN используются следующим образом:

- F - Обеспечивает синхронизацию.
- L - Отрегулировал среднее разрядное значение.
- E - Используемый для разрешения конфликта, когда несколько терминалов на пассивной шине борются за канал.
- A - Активирует устройства.
- S - Неназначенный.
- B1, B2 и D - Для пользовательских данных.

Устройства пользователя Нескольких сетей ISDN могут физически быть присоединены к одному каналу. Если два терминала передают одновременно, в этой конфигурации могут закончиться коллизии. Поэтому ISDN предоставляет функции для определения конкуренции ссылки. То, когда NT получает D, укусило от TE, он реагирует на бит в следующей позиции прибыли до уплаты налогов и процентов. TE ожидает, что следующий бит E для совпадения с его последним переданным D укусил.

Терминалы не могут передать в канал D, пока они сначала не обнаруживают определенное количество (указание на ""no signal"(сигнал отсутствует)") соответствие предустановленному приоритету. Если TE обнаруживает немного в эхе (E) канал, который отличается от его битов D, это должно прекратить передавать сразу. Этот простой способ гарантирует, что только один терминал может передать свое сообщение D когда-то. После успешной передачи сообщения D терминалу уменьшила его приоритет обязанность, обнаруживают более непрерывные перед передачей. Терминалы не могут повысить свой приоритет, пока все другие устройства на той же линии не имели возможность передать сообщение D. Телефонные подключения имеют более высокий приоритет, чем все другие сервисы, и сигнальная информация имеет более высокий приоритет, чем сведения, не относящиеся к передаче сигналов.

2-й уровень

Уровнем 2 протокола Сигнализации ISDN является Процедура получения доступа к каналу на канале D, также известном как LAPD. LAPD подобен High-Level Data Link Control (HDLC) и Сбалансированной процедуре доступа к каналу связи (LAPB). Как расширение сокращения LAPD указывает, это используется через канал D, чтобы гарантировать, что потоки контроля и сигнальной информации и получены должным образом. Формат кадра LAPD (см. рисунок 16-2) подобен тому из HDLC и, как HDLC, контрольное использование LAPD, информация и ненумерованный кадры. Протокол LAPD формально задан в Q.920 ITU-T и Q.921 ITU-T.

Рисунок 16-2: формат кадра LAPD

Флаг LAPD и Контрольные поля идентичны тем из HDLC. Поле адреса LAPD может быть или 1 или 2 байта длиной. Если расширенный бит адреса первого байта установлен, адрес составляет 1 байт; если это - "not set", адрес составляет 2 байта. Первый байт поля адреса содержит идентификатор точки доступа к сервису (SAPI), который определяет портал, в котором сервисы LAPD предоставлены Уровню 3. C/R укусил, указывает, содержит ли кадр

команду или ответ. Поле идентификатора оконечной точки терминала (TEI) определяет или сингл предельные или множественные терминалы. TEI всех указывает на широковещание.

Третий уровень

Две спецификации Уровня 3 используются для Сигнализации ISDN: ITU-T (раньше CCITT) Я 450 (также известный как Q.930 ITU-T) и ITU-T Я 451 (также известный как Q.931 ITU-T). Вместе, эти протоколы поддерживают от пользователя к пользователю, и соединения с пакетной коммутацией с коммутацией каналов. Множество установки вызова, прекращения вызова, информации и разных сообщений задано, включая НАСТРОЙКУ, ПОДКЛЮЧЕНИЕ, ВЫПУСК, СВЕДЕНИЯ О ПОЛЬЗОВАТЕЛЕ, ОТМЕНУ, СТАТУС и РАЗЪЕДИНЕНИЕ.

Эти сообщения функционально подобны предоставленным протоколом X.25 (см. Главу 19, "Устраняя неполадки Соединений X.25", для получения дополнительной информации). Рисунок 16-3, от ITU-T Я 451, показывает типичные этапы ISDN - вызова по коммутируемой линии.

Этапы ISDN - вызова по коммутируемой линии рисунка 16-3

Выходные данные Интерпретации команды show isdn status

Для обнаружения, что текущее положение ISDN - подключения между маршрутизатором и коммутатором телефонной компании используйте **команду show isdn status**. Два вида интерфейсов, которые поддерживаются этой командой, являются BRI и PRI.

```
3620-2#show isdn status Global ISDN Switchtype = basic-ni ISDN BRI0/0 interface dsl 0, interface
ISDN Switchtype = basic-ni Layer 1 Status: ACTIVE Layer 2 Status: TEI = 88, Ces = 1, SAPI = 0,
State = MULTIPLE_FRAME_ESTABLISHED TEI = 97, Ces = 2, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED Spid Status: TEI 88, ces = 1, state = 5(init) spid1 configured, no
LDN, spid1 sent, spid1 valid Endpoint ID Info: epsf = 0, usid = 0, tid = 1 TEI 97, ces = 2,
state = 5(init) spid2 configured, no LDN, spid2 sent, spid2 valid Endpoint ID Info: epsf = 0,
usid = 1, tid = 1 Layer 3 Status: 0 Active Layer 3 Call(s) Activated dsl 0 CCBs = 0 The Free
Channel Mask: 0x80000003
```

Таблица 16-5:-статус show isdn для BRI

Поле	Значение
Статус уровня 1: ДЕАКТИВИРОВАННЫЙ	Это указывает, что интерфейс BRI не видит сигнал на линии. Существует пять возможных причин для этого условия. • Интерфейс BRI является завершением. Или проверьте конфигурацию для **команды shutdown** под интерфейсом BRI или ищите административно выключенную индикацию от **команды show interface**. Используйте служебную программу конфигурации и не введите **завершение** под интерфейсом BRI. Введите **команду clear interface bri** в подсказку командной строки, чтобы

	удостовериться, что перезапущен интерфейс BRI. • Проблема существует с кабельным подключением. Необходимо будет заменить кабель. Удостоверьтесь, что вы используете сквозной кабель RJ-45. Для проверки кабеля держите концы кабеля RJ-45 рядом. Если контакты находятся в том же заказе, кабель является сквозным. Если заказ контактов инвертирован, кабель прокручен. Заменить кабель. • Порт ISDN BRI маршрутизатора мог бы потребовать устройства NT1. В ISDN NT1 является устройством, которое предоставляет интерфейс между коммутационным оборудованием центральной АТС и Customer Premises Equipment. Если маршрутизатор не имеет внутреннего NT1, получает и подключает NT1 с портом BRI. Удостоверьтесь, что BRI или терминальный адаптер присоединены к порту S/T NT1. См. документацию изготовителя для проверки нормальной работы внешнего NT1. • Линия не могла бы функционировать. Свяжитесь с носителем, чтобы подтвердить использование соединения и проверить параметры настройки типа коммутатора. • Удостоверьтесь, что маршрутизатор функционирует правильно. Если там неисправно или неисправное оборудование, замена по мере необходимости.
Статус уровня 2: Состояние = TEI_ASSIGNED	Проверьте параметр настройки типа коммутатора и SPID. Параметр коммутатора ISDN для конкретного интерфейса отвергнет глобальный параметр коммутатора. Состояние SPID укажет, принял ли коммутатор SPID (допустимый или недопустимый). Свяжитесь со своим поставщиком услуг для проверки установки, настроенной на

	маршрутизаторе. Для изменения настроек SPID используйте **ISDN** *spidn* команда настройки интерфейса. Где *n* равняется или 1 или 2, в зависимости от рассматриваемого канала. Используйте **эту команду с параметром no** для удаления указанного SPID. `isdn spidn spid-number [ldn]` `no isdn spidn spid-number [ldn]`**Описание синтаксиса:** `spid-number`Номер, определяющий сервис, на который вы подписались. Это значение назначено поставщиком Сервиса ISDN и обычно является 10-разрядным номером телефона с дополнительными цифрами. `ldn`(Необязательно) Местный абонентский номер (LDN), который является 7-разрядным номером, назначенным поставщиком услуг. Коммутатор в сообщении входящей настройки отправляет эту информацию. Если вы не включаете доступ локального каталога к коммутатору, разрешен, но другой канал B может не быть в состоянии получить входящие вызовы. Для наблюдения согласований уровня 2 между коммутатором и маршрутизатором используйте привилегированного **debug isdn q921** команды exec. Отладки q921 задокументированы в *Ссылку Команды отладки*. Отладки полагаются в большой степени на ресурсы ЦПУ, поэтому проявите осмотрительность при использовании их.

```
5200-1# show isdn status Global ISDN Switchtype = primary-5ess ISDN Serial0:23 interface dsl 0,
interface ISDN Switchtype = primary-5ess Layer 1 Status: ACTIVE Layer 2 Status: TEI = 0, Ces =
1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED Layer 3 Status: 0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0 The Free Channel Mask: 0x807FFFFF Total Allocated ISDN CCBs = 0 5200-1#
```

Если **команда show isdn status** не работает или не показывает PRI, попытайтесь использовать **команду show isdn service**. Удостоверьтесь**, что команда pri-group** появляется в конфигурации под контроллером T1/E1 в конфигурации. Если команда не присутствует, настройте контроллер с **командой pri-group**.

Ниже приводится пример конфигурации для маршрутизатора Cisco с контроллером T1/PRI с разделением каналов:

```
controller t1 0
framing esf
line code b8zs
pri-group timeslots 1-24
```

Таблица 16-6: статус show isdn для PRI

Поле	Значение
Статус уровня 1: ДЕАКТИВИРОВАННЫЙ	Это указывает, что интерфейс PRI не видит, что T1/E1 структурирует на линии. Рассмотрите следующие возможные причины для этого условия: • Интерфейс PRI является завершением. Или проверьте, что конфигурация для **команды shutdown** под serial0:23 взаимодействует или ищет административно выключенную индикацию от **команды show interface**. Используйте служебную программу конфигурации и не введите **завершение** под рассматриваемым интерфейсом. Введите *команду clear controller T1/E1 n* в подсказку командной строки, чтобы удостовериться, что перезапущен интерфейс PRI. • Проблема существует с кабельным подключением. Необходимо будет заменить кабель. Удостоверьтесь, что вы используете сквозной кабель RJ-45. Для проверки кабеля держите концы кабеля RJ-45 рядом. Если контакты находятся в том же заказе, кабель является сквозным. Если заказ контактов инвертирован, кабель прокручен. Заменить кабель. • Линия не могла бы функционировать. Свяжитесь с носителем, чтобы подтвердить использование соединения и проверить параметры настройки типа коммутатора. • Удостоверьтесь, что маршрутизатор функционирует правильно. Если там неисправно или неисправное оборудование, замена по мере необходимости.
Статус уровня 2: Состояние = TEI_ASSIGNE	Проверьте параметр настройки типа коммутатора. Параметр коммутатора ISDN для конкретного интерфейса отвергнет глобальный параметр

D	коммутатора. Проверьте, что T1/E1 настроен для соответствия с коммутатором поставщика (проблемы T1/E1 обсуждены в Главе 15). Для наблюдения согласований уровня 2 между коммутатором и маршрутизатором используйте привилегированного **debug isdn q921** команды exec. Отладки q921 задокументированы в *Ссылку Команды отладки*. Отладки полагаются в большой степени на ресурсы ЦПУ, поэтому проявите осмотрительность при использовании их.
Количество вызовов / Блоки управления вызовами в использовании / Общие Выделенные Контрольные блоки ВЫЗОВА ISDN	Эти номера указывают, сколько вызовов происходит, и количество ресурсов, которые выделены для поддержки тех вызовов. Если количество выделенных CCB выше, чем количество используемых CCB, полагайте, что могла бы быть проблема в выпуске CCB. Удостоверьтесь, что существуют доступные CCB для входящих вызовов.

Маршрутизация установления соединения по запросу: операции интерфейса программы для набора номера

Технология DDR является методом предоставления возможности подключения к WAN на экономичной, стандартной основе, или как основное соединение или как резервная копия для некоммутируемой последовательный ссылки.

Интерфейс номеронабирателя определен как любой интерфейс маршрутизатора, способный к размещению или приему вызова. Этот общий термин нужно отличить от термина **Интерфейс номеронабирателя** (с капиталом D), который обращается к логическому интерфейсу, настроенному для управления одним или более физическими интерфейсами маршрутизатора и который замечен в конфигурации маршрутизатора как interface Dialer X. От этой точки вперед, если не указано иное, мы будем использовать термин номеронабиратель в его обычном смысле.

Конфигурация интерфейса программы для набора номера прибывает в две разновидности: номеронабиратель на основе схемы (иногда называемый Унаследованным профилем DDR), и профили DDR. Какой метод, который вы используете, зависит от обстоятельств, при которых вы должны набрать подключение. Номеронабиратель на основе схемы DDR был сначала представлен в версии IOS 9.0, профилях DDR в версии IOS 11.2.

Инициирование набора

В его основе DDR является просто расширением маршрутизации, где*, вызывающие интересы пакет* маршрутизируются к интерфейсу номеронабирателя, инициируя набираемую попытку. Следующие разделы объясняют понятия, вовлеченные в определение представляющего интерес трафика, и объясняют маршрутизацию, используемую для подключений DDR.

Вызывающие интересы пакет

Содержательный термин, использованный для описания пакетов или трафика, который или инициирует набираемую попытку или, если набираемая ссылка будет уже активна, то перезагрузит счетчик простоя на интерфейсе номеронабирателя. Для пакета, который будут считать содержательным:

- пакет должен соответствовать критериям "разрешения", определенным access-list
- на access-list должен сослаться dialer-list, или пакет должен иметь протокол, который универсально разрешен dialer-list
- список номеронабирателя должен быть привязан к интерфейсу номеронабирателя при помощи dialer-group

Пакеты, как автоматически никогда полагают, не являются содержательными (по умолчанию). Определения содержательного пакета должны быть явно объявлены в маршрутизаторе или конфигурации сервера доступа.

Группа номеронабирателей

В конфигурации каждого интерфейса номеронабирателя на маршрутизаторе или сервере доступа, должна быть **команда dialer-group**. Если **команда dialer-group** не присутствует, нет никакого логического соединения между определениями содержательного пакета и интерфейсом. Синтаксис команды:

```
dialer-group [group number]
```

Номер группы является количеством группы доступа номеронабирателя, которой принадлежит определенный интерфейс. Эта группа доступа определена с **командой dialer-list**. Приемлемые значения являются ненулевыми, положительные положительные между 1 и 10.

Интерфейс может быть привязан к одиночной группе доступа номеронабирателя только; множественное присвоение dialer-group не позволено. Второе присвоение группы доступа номеронабирателя отвергнет первое. Группа доступа номеронабирателя определена с **командой dialer-group**. **Команда dialer-list** привязывает список доступа к группе доступа номеронабирателя.

Пакеты, которые совпадают с группой указанной программы набора номера, инициируют запрос подключения.

Адрес назначения (DA) пакета оценен против списка доступа, заданного в связанной **команде dialer-list**. Если это проходит, любой, который вызов инициируется (если никакое соединение не было уже установлено), или счетчик простоя перезагружен (если вызов в настоящее время связывается).

Список номеронабирателя

Команда глобальной кофигурации **dialer-list** используется для определения списка программы набора номеров DDR для управления набором номера протоколом, или сочетанием протокола и списком доступа. Вызывающие интересы пакет - те, которые совпадают с разрешением на уровне протокола или которые разрешены списком в **команде dialer-list**: *dialer-list dialer-group protocol protocol-name* **{разрешение | запрещает |** *list access-list-number* **| access-group}**

dialer-group является количеством группы доступа номеронабирателя, определенной в любой команде настройки интерфейса dialer-group.

protocol-name является одним из следующих ключевых слов протокола: AppleTalk, мост, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, VINES или xns.

permit – разрешает доступ к протоколу в целом.

deny – запрещает доступ к протоколу в целом.

список указывает, что список доступа будет использоваться для определения глубины детализации, более прекрасной, чем полный протокол.

access-list-number - Номера списка доступа, заданные в любом DECnet, Banyan VINES, IP, IPX Novell, или стандарте XNS или расширенных списках доступа, включая расширенную точку доступа к сервису IPX Novell (SAP) списки доступа и типы мостового соединения. Посмотрите Таблицу 16-7 для поддерживаемых типов списка доступа и номеров.

название списка фильтров *access-group* используется в **командах clns filter-set и clns access-group**.

Таблица 16-7: нумерация Access-List протоколом

Тип списка доступа	**Диапазон номера списка доступа (десятичное число)**
AppleTalk	600-699
Banyan VINES (стандарт)	1-100
Banyan VINES (расширился)	101-200
DEC Net	300-399
IP (стандарт)	1-99
IP (расширился)	100-199
IPX Novell (стандарт)	800-899
IPX Novell (расширился)	900-999
Прозрачное соединение	200-299
XNS	500-599

Список доступа

Для каждого сетевого протокола, который должен быть передан через набираемое соединение, может быть настроен список доступа. В целях управления затратами обычно выбираемо настроить список доступа для предотвращения определенного трафика, такого как обновления маршрута, от внедрения или поддержания на высоком уровне соединение. Обратите внимание на то, что, когда мы создаем списки доступа в целях определения содержательного и неинтересный трафик, мы не объявляем, что ненужные пакеты не могут пересечь набираемую ссылку. Мы просто указываем, что они не перезагрузят счетчик простоя, и при этом они не переведут соединение в рабочее состояние самостоятельно. Пока набираемое соединение подключено, ненужным пакетам все еще позволят течь через ссылку.

Например, маршрутизатору рабочий EIGRP как его протокол маршрутизации можно было настроить список доступа для объявления неинтересных пакетов EIGRP и весь другой содержательный IP - трафик:

```
access-list 101 deny eigrp any any
access-list 101 permit ip any any
```

Списки доступа могут быть настроены для всех протоколов, которые могли бы пересечь набираемую ссылку. Помните, что для любого протокола, поведение по умолчанию в отсутствие оператора **access-list permit** должно запретить весь трафик. Если не будет никакого списка доступа и никакой **команды dialer-list**, разрешающей протокол, то тот протокол будет неинтересным. В фактической практике, если нет никакого списка номеронабирателя для протокола, те пакеты не будут течь через ссылку вообще.

Пример - соединение всего этого

Со всеми элементами на месте, можно исследовать завершенный процесс, которым определен "содержательный" статус пакета. В данном примере IP и IPX являются протоколами, которые могут пересечь набираемую ссылку. Пользователь хочет препятствовать тому, чтобы широковещательные сообщения и обновления маршрута инициировали вызов или поддержали соединение.

```
!
interface async 1
 dialer-group 7
!
access-list 121 deny eigrp any any
access-list 121 deny ip any host 255.255.255.255
access-list 121 permit ip any any
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 903 permit -1
!
dialer-list 7 protocol ip list 121
dialer-list 7 protocol ipx list 903
!
```

Пакет должен быть разрешен операторами **access-list 121**, прежде, чем пересечь **interface async 1**, для рассмотрения *содержательным*. В этом случае пакеты EIGRP запрещены, как любые другие транслируемые пакеты, в то время как разрешен весь другой IP - трафик. Помните, что это не препятствует тому, чтобы пакеты EIGRP передали транзитом ссылку. Это только означает, что эти пакеты не будут перезагружать таймер простоя или инициировать набираемую попытку.

Точно так же **access-list 903** объявляет RIP IPX, SAP, и GNS запрашивает быть

неинтересным, в то время как весь другой трафик IPX является содержательным. Без этих инструкций deny вероятно никогда не снижалось бы набираемое соединение, и очень большой счет за телефонные услуги закончится, так как пакеты этих типов постоянно текут через сеть IPX.

С **dialer-group 7**, настроенным на асинхронном интерфейсе, мы знаем, что **dialer-list 7** необходим для связи фильтраций содержательного трафика (т.е. списки доступа) к интерфейсу. Один **оператор dialer-list** требуется (и *только один* может быть настроен) для каждого протокола, удостоверяясь, что номер списка номеронабирателя совпадает с номером группы номеронабирателей на интерфейсе.

Еще раз важно помнить, что *инструкции deny* в списках доступа, настроенных для определения представляющего интерес трафика***, не*** будут препятствовать тому, чтобы отклоненные пакеты пересекли ссылку.

Использование **номеронабирателя для отладки команды**, вы видите действие, которое инициирует набираемую попытку:

```
Dialing cause: Async1: ip (s=172.16.1.111 d=172.16.2.22)
```

Здесь мы видим, что IP - трафик с адресом источника 172.16.1.111 и адресом назначения (DA) 172.16.2.22 инициировал набираемую попытку на интерфейсном Async1.

Маршрутизация

После того, как определенный, вызывающие интересы пакет должны маршрутизироваться должным образом для вызова, который будет инициироваться. Процесс маршрутизации зависит от двух вещей: записи таблицы маршрутизации и взаимодействуют по который к маршрутизированным пакетам.

Интерфейсы - up/up (spoofing)

Для пакетов, которые будут маршрутизироваться к и через интерфейс, тот интерфейс должен быть up/up, как замечено в **выходных данных show interfaces**:

```
Montecito# show interfaces ethernet 0 Ethernet0 is up, line protocol is up Hardware is Lance,
address is . . .
```

Что происходит с интерфейсом номеронабирателя, который не связан? Если протокол не в порядке на интерфейсе, результат - то, что сам интерфейс не будет подключен. Маршруты, которые полагаются на тот интерфейс, будут сброшены от таблицы маршрутизации, и трафик не будет маршрутизироваться к тому интерфейсу. Результат состоит в том, что никакие вызовы не инициировались бы интерфейсом.

Решение противостоять этой возможности состоит в том, чтобы позволить **up/up (spoofing)** состояния для интерфейсов номеронабирателя. Любой интерфейс может быть настроен как интерфейс номеронабирателя. Например, Сериал или Асинхронный интерфейс могли быть превращены в номеронабирателя путем добавления **команды dialer in-band** или **dialer dtr** к конфигурации интерфейса. Эти линии являются ненужными для интерфейсов, которые являются по своей природе интерфейсом номеронабирателя (BRIs и PRI). Выходные данные для show interface будут похожи на это:

```
Montecito# show interfaces bri 0 BRI0 is up, line protocol is up (spoofing) Hardware is BRI
Internet address is . . .
```

Другими словами, интерфейс "симулирует" быть **up/up** так, чтобы связанные маршруты остались в силе и так, чтобы пакеты могли маршрутизироваться к интерфейсу.

Существуют обстоятельства, при которых интерфейс номеронабирателя не будет **up/up (spoofing)**. **Выходные данные show interface** могут показать интерфейс, как являющийся административно выключенным:

```
Montecito# show interfaces bri 0 BRI0 is administratively down, line protocol is down Hardware is BRI Internet address is . . .
```

Административно выключенный просто означает, что интерфейс был настроен с **командой shutdown**. Когда маршрутизатор загружен в самый первый раз, это - состояние по умолчанию любого интерфейса маршрутизатора. Для исправления этого используйте команду настройки интерфейса **никакое завершение**.

Интерфейс, как может также замечаться, находится в режиме ожидания:

```
Montecito# show interfaces bri 0 BRI0 is standby mode, line protocol is down Hardware is BRI Internet address is . . .
```

Это состояние указывает, что интерфейс был настроен как резервная копия для другого интерфейса. Когда соединение требует резервирования в случае сбоя, интерфейс номеронабирателя может быть установлен как резервная копия. Это выполнено путем добавления следующих команд к интерфейсу первичного соединения:

```
backup interface [interface]
backup delay [enable-delay] [disable-delay]
```

Как только **команда резервного интерфейса** была настроена, интерфейс, используемый, поскольку резервная копия будет помещена в режим ожидания до тех пор, пока основной интерфейс переходит к состоянию **вниз/вниз**. В то время интерфейс номеронабирателя, настроенный как резервная копия, перейдет **к состоянию up/up (спуфинг)**, ожидающему событие dial.

Статические маршруты и Floating Static Routes

Надежный способ к маршрутизированным пакетам к интерфейсу номеронабирателя со статичной маршрутизацией. Эти маршруты вручную введены в конфигурацию маршрутизатора или сервера доступа с командой:

маска префикса **ip route {***обращается* **|** *интерфейс***}** *[расстояние]*

префикс: Префикс маршрута IP для места назначения.

маска: Маска префикса для места назначения.

адрес: IP-адрес следующего перехода, который может использоваться для достижения сети назначения.

interface: Сетевой интерфейс для использования для исходящего трафика.

расстояние: (Необязательно) Административное расстояние. этот аргумент используется в плавающих статических маршрутах.

Статические маршруты используются в ситуациях, где набираемая ссылка является единственным соединением с удаленным узлом. Статический маршрут имеет значение

расстояния администрирования один (1), который делает, он предпочел по динамическим маршрутам тому же назначению.

С другой стороны, плавающие статические маршруты - т.е. статические маршруты с предустановленным административным расстоянием - как правило, используются в резервных сценариях DDR. В этих сценариях протокол динамической маршрутизации, таких как RIP или EIGRP, направляет пакеты через основное соединение.

Обычный статический маршрут (административное расстояние = 1) предпочтителен для любого EIGRP (административное расстояние = 90) или RIP (административное расстояние = 120). Даже если основной подключен и способен к проходящему трафику, статический маршрут заставляет пакеты маршрутизироваться через коммутируемую линию. Если, однако, статический маршрут будет настроен с административным расстоянием выше, чем тот из какого-либо из протоколов динамической маршрутизации в использовании на маршрутизаторе, то плавающий статический маршрут будет только использоваться в отсутствие "лучшего" маршрута - один с меньшим административным расстоянием.

Если Резервный DDR вызывается при помощи **команды резервного интерфейса**, ситуация является несколько другой. Поскольку интерфейс номеронабирателя остается в режиме ожидания, в то время как основной подключен, статический маршрут или плавающий статический маршрут могут быть настроены. Интерфейс номеронабирателя не попытается соединиться, пока основной интерфейс не идет **вниз/вниз**.

Для данного соединения количество статических (или плавающий статический) направляет необходимый, функция адресации на интерфейсах номеронабирателя. В случаях, где эти два интерфейса номеронабирателя (один на каждом из этих двух маршрутизаторов) совместно используют общую сеть или подсеть, требуется, как правило, только один статический маршрут. Это указывает к удаленной LAN с помощью адреса интерфейса номеронабирателя удаленного маршрутизатора как адрес следующего маршрутизатора.

Примеры

Пример 1: Набор является единственным соединением с помощью нумерованных интерфейсов. Один маршрут достаточен.

Рисунок 16-4: набор Использование нумерованных интерфейсов

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1
```

Пример 2: Набор является единственным соединением с помощью ненумерованных интерфейсов. Это может быть настроено со всего одним маршрутом, но распространено настроить два маршрута: маршрут хоста к интерфейсу LAN (локальной сети) на удаленном маршрутизаторе и маршруте к удаленной LAN через удаленный интерфейс LAN (локальной сети). Это сделано для предотвращения Layer3-to-Layer2 проблем сопоставления, которые могут привести к ошибкам инкапсуляции.

Если интерфейсы номеронабирателя на этих двух устройствах пронумерованы, но не в той же сети или подсети, этот метод также используется.

Рисунок 16-5: набор Использование ненумерованных интерфейсов

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1
ip route 192.168.10.1 255.255.255.255 BRI0
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 10.1.1.1 255.255.255.255 BRI0
```

Пример 3: Набор является резервным подключением с помощью нумерованных интерфейсов. Один плавающий статический маршрут требуется.

Рисунок 16-6: резервное Использование нумерованных интерфейсов

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2 200
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1 200
```

Пример 4: Набор является резервным подключением с помощью ненумерованных интерфейсов. Если интерфейсы номеронабирателя на этих двух устройствах пронумерованы, но не в той же сети или подсети, как в Примере 2 выше, также используется этот метод.

Рисунок 16-7: резервное Использование интерфейсов Unumbered

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1 200
ip route 192.168.10.1 255.255.255.255 BRI0 200
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1 200
ip route 10.1.1.1 255.255.255.255 BRI0 200
```

Схемы набора номеров

Номеронабиратель На основе схемы (Устаревший) DDR является мощным и всесторонним, но его масштабирование влияния ограничений и расширяемость. Номеронабиратель На основе схемы DDR основывается на статической привязке между для каждого назначения спецификация вызова и конфигурация физического интерфейса.

Однако Номеронабиратель На основе схемы DDR также имеет много сильных мест. Это поддерживает Frame Relay, CLNS ISO, LAPB, snapshot - маршрутизацию и все маршрутизируемые протоколы, которые поддерживаются на маршрутизаторах Cisco. По умолчанию Номеронабиратель На основе схемы DDR поддерживает быструю коммутацию.

При настройке интерфейса для исходящих вызовов одна схема набора номеров должна быть настроена для каждого удаленного назначения, и для каждого другого вызываемого номера в удаленном назначении. Например, если вы хотите многоканальное соединение PPP при наборе номера от ISDN BRI в другой интерфейс ISDN BRI, который имеет другой номер локального каталога для каждого из его B-каналов, вам нужна одна схема набора номеров для каждого из удаленных номеров:

```
!
interface bri 0
 dialer map ip 172.16.20.1 name Montecito broadcast 5551234
 dialer map ip 172.16.20.1 name Montecito broadcast 5554321
!
```

Заказ, в котором настроены схемы набора номеров, может быть важным. Если две или больше команды схемы набора номеров обратятся к тому же удаленному адресу, то маршрутизатор или сервер доступа будут судить их один за другим в заказе, пока это успешно не установит соединение

Примечание: IOS может динамично создать схемы набора номеров на маршрутизаторе, принимающем вызов. Схема набора номеров создана на основе проверенного имени пользователя и согласованного IP-адреса абонента. Динамические схемы набора номеров могут только быть замечены в выходных данных **команды show dialer map**. Вы не можете просмотреть их в рабочей конфигурации маршрутизатора или сервера доступа.

Синтаксис команды

Используйте следующую форму команды **конфигурации интерфейса схемы набора номеров** к:

- настройте последовательный интерфейс или интерфейс ISDN для вызова один или множественные узлы, или
- получите вызовы от множественных узлов.

Все варианты показываются в этой первой форме команды. Для удаления определенной записи схемы набора номера используйте **эту команду с параметром no**.

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
[broadcast] [modem-script modem-regexp] [system-script system-regexp]
[dial-string[:isdn-subaddress]]
```

Используйте следующую форму команды **схемы набора номеров** к:

- настройте последовательный интерфейс или интерфейс ISDN для заказывания телефонный разговор со множественными узлами, и
- аутентифицировать вызовы от множественных узлов.`dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64] [broadcast] [dial-string[:isdn-subaddress]]`

Используйте следующую форму команды **схемы набора номеров** для настройки последовательного интерфейса или интерфейса ISDN для поддержки мостового соединения.

```
dialer map bridge [name hostname] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

Используйте следующую форму команды **схемы набора номеров** для настройки асинхронного интерфейса для заказывания телефонный разговор с:

- одиночный узел, который требует системного сценария или это не имеет никакого назначенного сценария модема, или
- множественные узлы на отдельном канале, на составных строках, или на группе импульсного набора номера.`dialer map protocol next-hop-address [name hostname] [broadcast] [modem-script modem-regexp] [system-script system-regexp] [dial-string]`

Описание синтаксиса

- *протокол* **-** Ключевые слова протокола. Используйте одно из придерживающегося: **AppleTalk**, **мост**, **clns**, **decnet**, **ip**, **ipx**, **Novell ' s**, **снимок**, **VINES** или **xns**.
- *next-hop-address* - адрес использовал совпадать против адресов, к которым предназначены пакеты. Этот аргумент не используется с ключевым словом **протокола мостовой передачи**.
- **название** - (Необязательно) Указывает на удаленную систему, с которой связываются локальный маршрутизатор или сервер доступа. Используемый для аутентификации

удаленной системы на входящих вызовах.
- *host name-* (Необязательно) Имя с учетом регистра или ID удаленного устройства (обычно имя хоста). Для маршрутизаторов с интерфейсами ISDN *поле hostname* может содержать номер, который предоставляет ID вызывающей линии (в случаях, где Calling Line Identification, также называемый *CLI*, *идентификатором вызывающего абонента*, и *автоматическим определением номера (ANI)*, доступен).
- **SPC** - (Необязательно) Задает полупостоянное соединение между оборудованием заказчика и обменом. Это используется только в Германии для каналов между ISDN BRI и 1TR6 коммутатор ISDN и в Австралии для каналов между PRI ISDN и коммутатором TS-014.
- **скорость 56 | 64** - (Необязательно) Ключевое слово и значение, указывающее на скорость линии в килобитах в секунду для использования. Используемый для ISDN только. Скорость по умолчанию составляет 64 кбит/с.
- **широковещание** - (Необязательно) Указывает, что широковещательные сообщения должны быть переданы этому адресу.
- **modem-script** - (Необязательно) Указывает на сценарий модема, который будет использоваться для соединения (для асинхронных интерфейсов).
- *regexp модема* - (Необязательно) Регулярное выражение, к которому со сценарием модема совпадут (для асинхронных интерфейсов).
- **system-script** - (Необязательно) Указывает на системный сценарий, который будет использоваться для соединения (для асинхронных интерфейсов).
- *системный regexp* - (Необязательно) Регулярное выражение, к которому с системным сценарием совпадут (для асинхронных интерфейсов).
- *строка вызова [: подадрес ISDN]* (Необязательно) Номер телефона, передаваемый устройству установления соединения после распознавания пакетов с указанным адресом следующего узла, который совпадает с определенным списком доступа (и дополнительный номер подадреса, используемый для многоточечных соединений ISDN). Строка набора и Подадрес ISDN, если используется, должны быть последним элементом в командной строке.

Профили номеронабирателя

Примечание: В этом разделе термин "интерфейс номеронабирателя" относится к настраиваемому интерфейсу; не к физическому интерфейсу на маршрутизаторе или сервере доступа.

Реализация Профилей DDR DDR, представленного в версии IOS 11.2, основывается на разделении между логическим и конфигурацией физического интерфейса. Профили DDR также позволяют логическим и физическим конфигурациям быть связанными динамично на для каждого вызова основание.

Когда вы хотите сделать придерживающееся, методология Профилей DDR выгодна:

- совместно используйте интерфейс (ISDN, асинхронная, или синхронная последовательный), чтобы разместить или получить вызовы
- измените любую конфигурацию на основе для каждого пользователя (кроме инкапсуляции в первой фазе Профилей DDR)
- соедините многим назначениям
- избегите проблем расщепленного горизонта

Профили DDR позволяют конфигурации физических интерфейсов быть разделенной от логической конфигурации, требуемой для вызова, и они также позволяют логическим и физическим конфигурациям быть связанными динамично на для каждого вызова основание.

Профиль номеронабирателя состоит из следующих элементов:

- *Интерфейс номеронабирателя* (логический объект) конфигурация, включая одну или более строк набора (каждый из которых используется для достижения одной конечной подсети),
- *Класс схемы набора номеров*, который определяет все характеристики для любого вызова к указанной строке набора
- Упорядоченный *пул программ для набора номера* физических интерфейсов, которые будут использоваться интерфейсом номеронабирателя

Все переходящие вызовы или от той же конечной подсети используют тот же профиль DDR.

Конфигурация интерфейса программы для набора номера включает все параметры настройки, должен был достигнуть определенной конечной подсети (и любые сети, достигнутые через него). Множественные строки набора могут быть заданы для того же Интерфейса номеронабирателя; каждая строка набора может быть привязана к другому классу схемы набора номеров. Класс схемы набора номеров определяет все характеристики для любого вызова к указанной строке набора. Например, класс сопоставления для одного назначения мог бы задать скорость ISDN на 56 кбит/с. Класс сопоставления для другого назначения мог бы задать скорость ISDN на 64 кбит/с.

Каждый Интерфейс номеронабирателя использует пул программ для набора номера, который является пулом физических интерфейсов, упорядоченных на основе приоритета, назначенного на каждый физический интерфейс. Физический интерфейс может принадлежать составным пулам программ набора номеров с конкуренцией, решаемой приоритетом. ISDN BRI и интерфейсы PRI могут установить предел для минимума и максимального числа каналов B, зарезервированных любыми пулами программ для набора номера. Канал, зарезервированный пулом программ для набора номера, остается простаивающим, пока трафик не направлен к пулу.

Когда Профили DDR используются для настройки DDR, физический интерфейс не имеет никаких параметров конфигурации кроме инкапсуляции и пулов программ для набора номера, которым принадлежит интерфейс.

Примечание: Предыдущий абзац имеет одно исключение. Команды, которые применяются перед аутентификацией, завершены, должен быть настроен на медосмотре (или BRI или PRI) интерфейс а не на Профиле DDR. Профили DDR не копируют команды проверки подлинности PPP (или команды LCP) к физическому интерфейсу.

Рисунок 16-8 показывает типичное приложение профилей DDR. Маршрутизатор A имеет интерфейс номеронабирателя 1 для маршрутизации по требованию с подсетью 1.1.1.0 и интерфейса номеронабирателя 2 для маршрутизации по требованию с подсетью 2.2.2.0. IP-адрес для интерфейса номеронабирателя 1 является своим адресом как узлом в сети 1.1.1.0. В то же время тот IP-адрес служит IP-адресом физических интерфейсов, используемых интерфейсом номеронабирателя 1. Точно так же IP-адрес для интерфейса номеронабирателя 2 является своим адресом как узлом в сети 2.2.2.0.

Рисунок 16-8: типичное приложение профилей DDR

Интерфейс номеронабирателя использует только один пул программ для набора номера. Физический интерфейс, однако, может быть участником одного или нескольких пулов программ для набора номера, и пул программ для набора номера может иметь несколько физических интерфейсов в качестве участников.

Рисунок 16-9 иллюстрирует отношения среди понятий интерфейса номеронабирателя, пула программ для набора номера и физических интерфейсов. Интерфейс номеронабирателя 0 пулов программ для набора номера использования 2. BRI 1 физического интерфейса принадлежит пулу программ для набора номера 2 и имеет определенный приоритет в пуле. BRI 2 физического интерфейса также принадлежит пулу программ для набора номера 2. Поскольку конкуренция решена на основе уровней приоритета физических интерфейсов в пуле, BRI 1 и BRI 2 нужно назначить другие приоритеты в пуле. Возможно, BRI 1 является присвоенным приоритетом 100, и BRI 2 является присвоенным приоритетом 50 в пуле программ для набора номера 2 (приоритет 50 выше, чем приоритет 100). BRI 2 имеет более высокий приоритет в пуле, и его вызовы будут размещены сначала.

Рисунок 16-9: отношения среди интерфейсов номеронабирателя, пулов программ для набора номера и физических интерфейсов

Шаги конфигурации профиля DDR

Команда	Цель
interface dialer number	Создайте Интерфейс номеронабирателя.
ip address address mask	Укажите IP-адрес и маску интерфейса номеронабирателя в качестве узла в сети назначения, который необходимо вызвать.
encapsulation ppp	Укажите инкапсуляцию PPP.
dialer remote-name username	Задайте название Аутентификации CHAP удаленного маршрутизатора.
dialer string dial-string class class-name	Задайте удаленное назначение для вызова и класс сопоставления, определяющий характеристики вызовов данного назначения.
номеронабиратель *poolnumber*	Задайте пул набора для вызовов в этом направлении.
номер группы dialer-group	Назначьте интерфейс номеронабирателя группе номеронабирателей.
dialer-list dialer-group protocol protocol-name **{разрешение | запрещает |** *list access-list-number***}**	Задайте список доступа номером списка или протоколом и номером списка для определения "содержательных" пакетов, которые могут инициировать вызов.

Операции PPP

Протокол PPP является бесспорно наиболее распространенным транспортным протоколом канального уровня, полностью узурпировав SLIP как предпочтительный протокол для набора (и во многих случаях, ненабора) синхронный и асинхронные последовательные соединения. PPP был первоначально определен в 1989 RFC 1134, который был с тех пор сделан устаревшим серией достижения высшей точки RFC (с этой записи) в RFC1661. Существуют также многочисленные RFC, которые определяют элементы протокола, такие как RFC1990 (Протокол PPP Multilink), RFC2125 (Протокол Распределения пропускной способности PPP), и многие другие. Онлайновый репозиторий RFC может быть найден в:

http://www.ietf.org/rfc.html

Возможно, лучшее определение PPP может быть найдено в RFC1661, который сообщает:

Протокол PPP предоставляет стандартный метод для переноса многопротокольных датаграмм по каналам типа точка-точка. PPP состоит из трех основных компонентов:

1. Метод для инкапсуляции многопротокольных датаграмм.
2. Протокол управления каналом (LCP) для установления, настройки и тестирования подключения канального уровня.
3. Семейство Протоколов управления сетью (NCP) для установления и настройки других протоколов сетевого уровня.

Стадии согласования PPP

Согласование PPP состоит из трех фаз: Протокол управления каналом (LCP), Аутентификация и Протокол управления сетью (NCP). Каждый продолжается в заказе, после установления асинкса или ISDN - подключения.

LCP

PPP не придерживается модели клиент/сервер. Все соединения являются одноранговыми. Поэтому, когда существует абонент и получатель, оба конца двухточечного соединения должны договориться о согласованных протоколах и параметрах.

Когда согласование начинается, каждый из узлов, желающих установить PPP - подключение, должен отправить Настраивать Запрос (замеченный в **debug ppp negotiation** и упомянутый после этого как CONFREQ). Включенный в CONFREQ любые опции, которые не являются по умолчанию ссылки. Они часто включают Maximum Receive Unit (MRU), Async Control Character Map (ACCM), Протокол аутентификации (AuthProto) и Системный код. Также замеченный Maximum Receive Reconstructed Unit (MRRU) и Дискриминатор оконечной точки (EndpointDisc), используемый для Протокола PPP.

Существует три возможных ответа к любому CONFREQ:

- Настраивание - Подтверждает (CONFACK), должен быть выполнен, если узел распознает опции и соглашается на значения, замеченные в CONFREQ.
- Configure-Reject (CONFREJ) должен быть передан, если какая-либо из опций в CONFREQ не распознана (например, некоторые параметры, зависящие от поставщика)

или если значения для какой-либо из опций были явно запрещены в конфигурации узла.
- Настраивать-отрицательное-квитирование (CONFNAK) должно быть передано, если все опции в CONFREQ распознаны, но значения не приемлемы для узла.

Два узла продолжают обмениваться CONFREQ, CONFREJ и CONFNAK, пока каждый не передает CONFACK, пока набираемое соединение не сломано, или до один или оба из узлов, указывает, что не может быть завершено согласование.

Authentication

После успешного завершения согласования LCP и достижения соглашения по AuthProto, следующий шаг является аутентификацией. Аутентификация, в то время как не обязательный на RFC1661, настоятельно рекомендована на всех набираемых соединениях. В некоторых случаях это - требование для правильной работы; Профили DDR, являющиеся подходящим примером.

Этими двумя принципиальными типами аутентификации в PPP является Протокол аутентификации пароля (PAP) и Протокол аутентификации по квитированию вызова (CHAP), определенный RFC1334 и обновленный RFC1994.

PAP является более простыми из этих двух, но менее безопасен, потому что открытый пароль передается через набираемое соединение. CHAP более безопасен, потому что открытый пароль никогда не передается через набираемое соединение.

PAP может быть необходимым в одной из следующих сред:

- Большая установленная база клиентских приложений, не поддерживающих протокол аутентификации CHAP
- Несовместимость между различными реализациями изготовителя CHAP

При обсуждении аутентификации полезно использовать термины "запрашивающая сторона" и "средство проверки подлинности" для различения ролей, которые играют устройства с обоих концов соединения, хотя любой узел может действовать в любой роли. "Запрашивающая сторона" описывает устройство, которое запрашивает доступ к сети и предоставляет информацию для аутентификации; "средство проверки подлинности" проверяет законность информации для аутентификации и или позволяет или запрещает соединение. Когда подключение DDR делается между маршрутизаторами, обоим узлам свойственно действовать в обеих ролях.

PAP

PAP довольно прост. После успешного завершения согласования LCP запрашивающая сторона неоднократно передает свое сочетание имени пользователя и пароля через ссылку, пока средство проверки подлинности не отвечает подтверждением или пока не разорвана связь. Средство проверки подлинности может разъединить ссылку, если это решает, что сочетание имени пользователя и пароля не допустимо.

CHAP

CHAP несколько более сложен. Средство проверки подлинности передает вызов запрашивающей стороне, которая тогда отвечает значением. Это значение вычислено при помощи функции "однонаправленного хэширования" для хеширования проблемы и пароля

CHAP вместе. Итоговое значение передается средству проверки подлинности наряду с Именем хоста CHAP запрашивающей стороны (который может отличаться от его действительного имени хоста) в *ответном сообщении*.

Средство проверки подлинности читает имя хоста в ответном сообщении, ищет ожидаемый пароль для того имени хоста, и затем вычисляет значение, это ожидает запрашивающую сторону, передаваемую в ее ответе путем выполнения той же хэш-функции выполненная запрашивающая сторона. Если итоговые значения совпадают, аутентификация успешна. Сбой должен привести к разъединению.

AAA

Сервис аутентификации, авторизации и учета (AAA), такой как TACACS + или RADIUS, может использоваться в выполнении PAP или CHAP.

NCP

После успешной аутентификации начинается фаза NCP. Как в LCP, узлы обмениваются CONFREQ, CONFREJ, CONFNAK и CONFACK. Однако в этой фазе согласования, элементы, являющиеся договорным, имеют отношение к протоколам высшего уровня - IP, IPX, Мостовое соединение, CDP, и так далее. Один или больше этих протоколов может быть выполнен согласование. Поскольку это обычно используется, и потому что другие протоколы работают почти такой же формой, Протокол управления протоколом IP (IPCP), определенный в RFC1332, является фокусом этого обсуждения. Другие подходящие RFC включают, но не ограничены:

- RFC1552 (протокол управления IPX)
- RFC1378 (протокол управления AppleTalk)
- RFC1638 (соединяющий протокол управления)
- RFC1762 (протокол управления DECnet)
- RFC1763 (протокол управления VINES)

Кроме того, о Протоколе обнаружения Cisco протоколе управления (CDPCP) можно выполнить согласование во время NCP, хотя это не распространено. Специалисты службы технической поддержки Cisco будут обычно советовать, чтобы команда no cdp enable быть настроенной на любом и всех интерфейсах номеронабирателя для предотвращения пакетов CDP, поддерживающих призыв неопределенно.

Ключевым элементом, согласуемым по протоколу IPCP, является адрес каждой точки одноранговой соединения. Каждый из узлов находится в одном из двух возможных состояний; либо он имеет IP-адрес, либо нет. Если узел уже будет иметь адрес, то он передаст тот адрес в CONFREQ к другому узлу. Если адрес будет приемлем для другого узла, то CONFACK будет возвращен. Если адрес не будет приемлем, то ответ будет CONFNAK, содержащим адрес для узла для использования.

Если узел не будет иметь никакого адреса, то он передаст CONFREQ с адресом 0.0.0.0. Это говорит другому узлу назначать адрес, который выполнен передачей CONFNAK с соответствующим адресом.

О других опциях можно выполнить согласование в IPCP. Обычно замечаемый основной и вторичные адреса для Сервера доменных имен и Сервера имен NETBIOS, как описано в Информационном RFC1877. Протокол сжатия IP (RFC1332) также распространен.

Дополнительные стандарты PPP

Дополнительные стандарты PPP включают протокол PPP, PPP мультишасси и виртуальные профили.

Multilink PPP

Многоканальный протокол "точка-точка" (MLP) функция предоставляет функциональные возможности балансировки нагрузки по несколько каналов глобальной сетям. В то же время это предоставляет совместимость нескольких поставщиков, фрагментацию пакета и надлежащее упорядочение и расчет нагрузки на обоих входящих и исходящих трафиках. Внедрение Cisco Протокола PPP поддерживает фрагментацию и спецификации упорядочения пакетов в RFC1717.

Протокол PPP позволяет пакетам быть фрагментированными. Эти фрагменты могут быть переданы в то же время по множественным каналам связи точка-точка к тому же удаленному адресу. Сложные соединения подходят в ответ на порог загрузки номеронабирателя, который вы определяете. Загрузка может быть вычислена на входящий трафик, исходящий трафик, или на также, по мере необходимости для трафика между определенными узлами. MLP предоставляет полосу по требованию и уменьшает задержку передачи через каналы WAN.

Протокол PPP перерабатывает следующие типы интерфейса (одиночный или множественный), которые настроены для поддержки и групповых номеров установления соединения по запросу и инкапсуляции PPP:

- асинхронные последовательные интерфейсы
- BRIs
- PRI

!--- конфигурацию

Для настройки Протокола PPP на асинхронных интерфейсах вы настраиваете асинхронные интерфейсы для поддержки DDR и инкапсуляции PPP. Вы тогда настраиваете Интерфейс номеронабирателя для поддержки инкапсуляции PPP, полосы по требованию и Протокола PPP. В некоторый момент, однако, добавление большего количества асинхронных интерфейсов не улучшает производительность. Со стандартным размером MTU Протокол PPP должен поддержать три асинхронных интерфейса с помощью модемов V.34. Однако пакеты могли бы иногда отбрасываться, если MTU является маленьким или если происходят большие пакеты коротких фреймов.

Для включения Протокола PPP на одиночном ISDN BRI или интерфейсе PRI вы не обязаны определять группу импульсного набора номера отдельно, потому что интерфейсы ISDN являются группами импульсного набора номера по умолчанию. Если вы не используете процедуры проверки подлинности PPP, ваша телефонная служба должна передать информацию об идентификаторе вызывающего абонента.

Номер порога нагрузки требуется. Для примера настройки Протокола PPP на одиночном интерфейсе ISDN BRI посмотрите *Пример протокола PPP на Одном Интерфейсе ISDN* ниже.

Когда Протокол PPP настроен, и вы хотите, чтобы многоканальное соединение было связано неопределенно, использовало команду **таймаута простоя программы для набора номера** для установки очень высокого счетчика простоя. **Команда dialer-load threshold 1** не поддерживает многоканальное соединение ссылок *n* связанным неопределенно, и **команда dialer-load threshold 2** не поддерживает многоканальное соединение двух ссылок связанным неопределенно.

Для включения Протокола PPP на BRI нескольких сетей ISDN или интерфейсах PRI вы устанавливаете ротацию Номеронабирателя, взаимодействуют и настраивают его для Протокола PPP. Вы тогда настраиваете BRIs отдельно и добавляете их каждый к тому же групповому номеру. Посмотрите *Пример протокола PPP на Нескольких интерфейсах ISDN* ниже.

Пример протокола PPP на одном интерфейсе ISDN

Следующий пример включает Протокол PPP на интерфейсе BRI 0. Когда один BRI настроен, никакая настройка группы телефонной связи программы для набора номера не требуется (интерфейс ISDN является групповым номером по умолчанию).

```
interface bri 0
ip address 171.1.1.7 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 30
 dialer load-threshold 40 either
 dialer map ip 172.16.20.2 name Goleta 5551212
 dialer-group 1
 ppp authentication pap
 ppp multilink
```

Пример протокола PPP на нескольких интерфейсах ISDN

Следующий пример настраивает несколько сетей ISDN BRIs для принадлежности той же группе импульсного набора номера для Протокола PPP. Используйте команду **группы импульсного набора номера** для присвоения каждой ISDN BRIs к той группе импульсного набора номера, которая должна совпасть с количеством Интерфейса номеронабирателя (номер 0 в этом случае).

```
interface BRI0
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface BRI1
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface Dialer0
 ip address 172.16.20.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 172.16.20.2 name Goleta broadcast 5551212
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

PPP многоблочного мультиканального протокола

Протокол PPP предоставляет возможность разделения и перекомпоновок пакетов к одиночной конечной системе через логический канал (также названный *связкой (bundle)*) сформированный сложными соединениями. Протокол PPP предоставляет полосу по требованию и уменьшает задержку передачи через каналы WAN.

Протокол PPP с использованием нескольких шасси и нескольких каналов (MMP), с другой стороны, предоставляет дополнительную возможность ссылок для завершения в нескольках маршрутизаторов с другими удаленными адресами. MMP может также обработать оба аналоговых и цифровых трафика.

Эта функциональность предназначена для ситуаций, в которых существуют большие бассейны пользователей с наборным телефонным доступом, в которых сервер одиночного доступа не может предоставить достаточно портов входящего (телефонного) соединения. MMP позволяет компаниям предоставлять одиночный телефонный номер модема своим пользователям и применять то же решение аналога и цифровых вызовов. Эта функция позволяет интернет-провайдерам, например, выделять одиночный номер в группе телефонной связи ISDN нескольким PRI ISDN через несколько маршрутизаторов.

Для полного описания команд MMP, на которые ссылаются здесь, обратитесь к *Справочнику по командам Решений для Вызова cisco*. Для поиска документации по другим командам, встречающимся в данной главе см. указатель справочника по командам или произведите поиск на сайте.

MMP поддерживается на платформах серии Cisco 7500, 4500 и 2500 и на синхронном последовательный, асинхронном последовательный, ISDN BRI, PRI ISDN и Интерфейсах номеронабирателя.

MMP не требует изменения конфигурации коммутаторов телефонной компании.

!--- конфигурацию

Маршрутизаторы или серверы доступа настроены для принадлежности группам узлов, названных *стеками групп*. Все участники стека групп являются узлами; стекам групп не нужен постоянный ведущий маршрутизатор. Любой член группы стека может ответить на звонки, прибывающие из номера одиночного обращения, который обычно является группой последовательного поиска PRI ISDN. Вызовы могут войти от устройств удаленного пользователя, таких как маршрутизаторы, модемы, адаптеры терминала ISDN или Карты ПК.

Как только соединение установлено с одним участником *стека групп*, тот участник владеет вызовом. Если повторный звонок входит от того же клиента, и другой маршрутизатор отвечает на звонок, маршрутизатор устанавливает туннель и вперед все пакеты, принадлежащие вызову к маршрутизатору, который владеет вызовом. Процесс установления туннеля и перевода вызовов через него к маршрутизатору, который владеет вызовом, иногда вызывают*, проектируя Канал "PPP" ведущему устройству вызова*.

Если больше мощного маршрутизатора доступно, он может быть настроен в качестве участника стека групп, и другие члены группы стека могут установить туннели и перевести все вызовы к нему. В таком случае другие члены группы стека просто отвечают на звонки, и перенаправление трафика к более мощному *разгружают* маршрутизатор.

Примечание: С большой задержкой линии глобальной сети (WAN) между членами группы стека могут сделать операцию стека групп неэффективной.

Обработка вызова MMP, предложение цены и функционирования переадресации Уровня 2 в стеке групп продолжаются следующим образом. Это также показывают на рисунке 16-10.

1. Когда первый вызов входит к стеку групп, маршрутизатор ответы.
2. В предложении цены, маршрутизатор wins, потому что это уже имеет вызов. Маршрутизатор A становится *ведущим устройством вызова* для того сеанса с удаленным устройством. Маршрутизатор A можно было бы также назвать *хостом основного интерфейса пучка*.
3. Когда удаленному устройству, которое инициировало вызов, нужно больше пропускной способности, это выполняет второй вызов Протокола PPP группе.
4. Когда повторный звонок входит, маршрутизатор D отвечает на него и сообщает стеку групп. Маршрутизатор wins предложение цены, потому что это уже обрабатывает сеанс через то удаленное устройство.
5. Маршрутизатор D устанавливает туннель к маршрутизатору A и вперед необработанным данным PPP к маршрутизатору A.
6. Маршрутизатор A повторно собирает и повторно упорядочивает пакеты.
7. Если больше вызовов входит к маршрутизатору D, и они также принадлежат маршрутизатору A, туннель между A и D увеличивается для обработки добавляемого трафика. Маршрутизатор D не устанавливает дополнительный туннель к A.
8. Если больше звонков входит и отвечено каким-либо другим маршрутизатором, тот маршрутизатор также устанавливает туннель к A и вперед необработанным данным PPP.
9. Повторно собранные данные передают корпоративной сети, как будто это все проникло через одно физическое соединение.

Рисунок 16-10: типичный сценарий протокола PPP многоблочного мультиканального протокола

В отличие от предыдущего рисунка, рисунок 16-11 обладает разгружать маршрутизатором. Серверы доступа, которые принадлежат стеку групп, отвечают на звонки, устанавливают туннели и переводят вызовы к Маршрутизатору Cisco 4700, который выигрывает предложение цены и является ведущим устройством вызова для всех вызовов. Cisco 4700 повторно собирает и повторно упорядочивает все пакеты, входящие через стек групп.

Рисунок 16-11: PPP многоблочного мультиканального протокола с разгружать маршрутизатором как член группы стека

Примечание: Можно создать стеки групп с помощью другого сервера доступа, коммутации и платформ маршрутизатора. Однако универсальные серверы доступа, такие как Cisco AS5200 не должны быть объединены с ISDN. Это должно только быть сделано с серверами доступа такой как 4x00 платформа. Поскольку вызовы от центральной АТС выделены в произвольном способе, эта комбинация могла привести к аналоговому вызову, отправляемому цифровому единственному серверу доступа, который не будет в состоянии обработать вызов.

Поддержка MMP на группе маршрутизаторов требует, чтобы каждый маршрутизатор был настроен для поддержки придерживающегося:

- Multilink PPP
- Протокол приглашения стека групп (SGBP)
- Виртуальный шаблон, используемый для клонирования конфигурации интерфейса для поддержки MMP

Виртуальные профили

Виртуальные профили являются уникальным приложением Протокола PPP, которое может создать и настроить интерфейс виртуального доступа динамично, когда входящий (телефонный) вызов получен, и разъедините интерфейс динамично, когда заканчивается вызов. Виртуальные профили работают с прямым PPP и с Протоколом PPP (MLP).

Сведения о конфигурации для интерфейса виртуального доступа Виртуальных профилей могут прибыть из интерфейса виртуального шаблона, или из конфигурации конкретного пользователя, сохраненной на аутентификации, авторизации и учете (AAA) или обоих.

Конфигурация user-specific AAA, используемая Виртуальными профилями, является *конфигурацией интерфейса* и загружена во время согласований LCP. Другая функция, названная Настройкой на базе отдельных пользователей, также использует сведения о конфигурации, полученные от AAA-сервера. Однако Настройка на базе отдельных пользователей использует *конфигурацию сети* (такую как списки доступа и фильтры маршрута) загруженный во время согласований NCP.

Два правила управляют конфигурацией интерфейса виртуального доступа интерфейсами виртуального шаблона Виртуальных профилей и конфигурациями AAA:

- Каждое приложение для виртуального доступа может иметь, самое большее, один шаблон, от которого можно клонироваться. Однако это может иметь множества конфигураций AAA (проверка подлинности, авторизация и учет), от которых можно клонироваться (Сведения AAA виртуальных профилей и AAA настройка на базе отдельных пользователей, которая в свою очередь могла бы включать протоколы конфигурации для нескольких).
- Когда Виртуальные профили настроены виртуальным шаблоном, его шаблон имеет более высокий приоритет, чем какой-либо другой виртуальный шаблон.

Посмотрите "Совместимость с Другими Функциями телефонной связи Cisco" раздел ниже для описания последовательностей возможной конфигурации, которые зависят от присутствия или отсутствия MLP или другой функцией виртуального доступа, которая клонирует интерфейс виртуального шаблона.

Эта функция работает на всех платформах Cisco IOS тот MLP поддержки.

Для полного описания команд, упомянутых в этом разделе, обратитесь к "главе" Команд Виртуальных профилей в *Набираемом Справочнике по командам Решений* в наборе документации по Cisco IOS. Для определения местоположения документации других команд, которые появляются в этой главе можно использовать Алфавитный указатель справочника по командам или искать онлайн.

Общие сведения

Этот раздел представляет общие сведения о Виртуальных профилях, чтобы помочь вам

понимать это приложение, прежде чем вы начнете настраивать его.

Ограничения

Мы рекомендуем, чтобы ненумерованные адреса использовались в интерфейсах виртуального шаблона, чтобы гарантировать, что дублирования сетевого адреса не созданы на интерфейсах виртуального доступа.

Предварительные условия

Использование информации о конфигурации интерфейса AAA (проверка подлинности, авторизация и учет) для отдельных пользователей с Виртуальными профилями требует, чтобы маршрутизатор был настроен для AAA, и требует, чтобы AAA-сервер имел пары значение-атрибут конфигурации интерфейса конкретного пользователя. Соответствующие пары значение-атрибут (на сервере RADIUS) начинаются следующим образом:

```
cisco-avpair = "lcp:interface-config=...",
```

Информацией, которая придерживается равного сигнала (=), могла быть любая команда настройки Интерфейса Cisco IOS. Например, линия могла бы быть придерживающимся:

```
cisco-avpair = "lcp:interface-config=ip address 200.200.200.200
255.255.255.0",
```

Использование интерфейса виртуального шаблона с Виртуальными профилями требует, чтобы виртуальный шаблон был определен в частности для Виртуальных профилей.

Совместимость с другими функциями телефонной связи Cisco

Виртуальные профили взаимодействуют с DDR Cisco, Протокол PPP (MLP) и номеронабиратели, такие как ISDN.

Конфигурация DDR физических интерфейсов

Когда никакое другое приложение интерфейса виртуального доступа не настроено, виртуальные профили полностью взаимодействуют с физическими интерфейсами в следующих состояниях конфигурации DDR:

- Профили DDR настроены для интерфейса. Профиль DDR используется вместо конфигурации Виртуальных профилей.
- DDR не настроен на интерфейсе. Виртуальные профили отвергают текущую конфигурацию.
- Унаследованный профиль DDR настроен на интерфейсе. Виртуальные профили отвергают текущую конфигурацию.

Примечание: Если интерфейс номеронабирателя используется (включая любого Номеронабирателя ISDN), его конфигурация используется на физическом интерфейсе вместо конфигурации Виртуальных профилей.

Эффект протокола PPP на конфигурацию интерфейса виртуального доступа

Как показано в таблице 16-8, точная конфигурация интерфейса виртуального доступа зависит от следующих трех факторов:

- Настроены ли Виртуальные профили Виртуальным шаблоном, AAA, обоими, или ни одним. Эти состояния показывают как "VT VP только", "AAA VP только", "VT VP и AAA VP", и "Никакой VP вообще", соответственно, в таблице.
- Присутствие или отсутствие интерфейса номеронабирателя.
- Присутствие или отсутствие MLP. Метка столбца "MLP" является заместителем для любой функции виртуального доступа, которая поддерживает MLP и клоны от интерфейса виртуального шаблона.

В Таблице 16-8, "Многоканальный VT" означает, что интерфейс виртуального шаблона клонирован*, если* вы определены для MLP или функции виртуального доступа, которая использует MLP.

Таблица 16-8: последовательность клонирования конфигурации виртуальных профилей

Конфигурация виртуальных профилей	MLP никакой номеронабиратель	Номеронабиратель MLP	Никакой MLP никакой номеронабиратель	Никакой номеронабиратель MLP
VT VP только	VT VP	VT VP	VT VP	VT VP
AAA VP только	(Многоканальный VT) AAA VP	(Многоканальный VT) AAA VP	AAA VP	AAA VP
VT VP и AAA VP	AAA VP VT VP	AAA VP VT VP	AAA VP VT VP	AAA VP VT VP
Никакой VP вообще	(Многоканальный VT)	Номеронабиратель	Никакой действительный интерфейс доступа не создан.	Никакой действительный интерфейс доступа не создан.

Порядок пунктов в любой ячейке таблицы важен. Где VT VP показывают выше AAA VP, это означает, что сначала виртуальный шаблон Виртуальных профилей клонирован на интерфейсе, и затем конфигурация интерфейса AAA для пользователя применена к нему. Конфигурация интерфейса AAA (проверка подлинности, авторизация и учет) для отдельных пользователей добавляет к конфигурации и отвергает любой конфликтный физический интерфейс или команды настройки виртуального шаблона.

Совместимость с другими Функциями то Использование Виртуальные шаблоны

Виртуальные профили также взаимодействуют с приложениями для виртуального доступа, которые клонируют интерфейс виртуального шаблона. Каждое приложение для виртуального доступа может иметь, самое большее, один шаблон, от которого можно клонироваться, но может клонироваться от множеств конфигураций AAA (проверка подлинности, авторизация и учет).

Взаимодействие между Виртуальными профилями и другими приложениями виртуального шаблона следующие:

- Если Виртуальные профили включены, и виртуальный шаблон определен для него, виртуальный шаблон Виртуальных профилей используется.
- Если Виртуальные профили настроены одним только AAA (никакой виртуальный шаблон не определен для Виртуальных профилей), виртуальный шаблон для другого приложения для виртуального доступа (VPDN, например) может быть клонирован на интерфейс виртуального доступа.
- Виртуальный шаблон, если таковые имеются, клонирован к интерфейсу виртуального доступа перед конфигурацией AAA Виртуальных профилей или AAA настройкой на базе отдельных пользователей. AAA настройка на базе отдельных пользователей, если используется, применена в последний раз.

Терминология

Следующие новые или редкие термины использованы в этой главе:

Пара значение-атрибут: параметр конфигурации на AAA-сервере; часть пользовательской конфигурации, которую AAA-сервер передает к маршрутизатору, в ответ на определяемые пользователем запросы авторизации. Маршрутизатор интерпретирует каждую пару значение-атрибут как команду настройки маршрутизатора Cisco IOS и применяет пары значение-атрибут в заказе. В этой главе термин пара значение-атрибут относится к параметру конфигурации интерфейса на сервере RADIUS.

Пара значение-атрибут конфигурации интерфейса для Виртуальных профилей может принять форму, такую как это:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
```

клонирование: Создание и настройка интерфейса виртуального доступа путем применения команд настройки от определенного виртуального шаблона. Виртуальный шаблон является источником информации об основном пользователе и сведений зависящие от маршрутизатора. Результатом клонирования является интерфейс виртуального доступа, настроенный со всеми командами в шаблоне.

интерфейс виртуального доступа: Экземпляр уникального виртуального интерфейса, который создан динамично и существует временно. Интерфейсы виртуального доступа могут быть созданы и настроены по-другому другими приложениями, такими как Виртуальные профили и виртуальные частные коммутируемые сети.

интерфейс виртуального шаблона: Конфигурация общего интерфейса для некоторых пользователей или для определенной цели, плюс сведения зависящие от маршрутизатора. Это принимает форму списка команд Интерфейса Cisco IOS, которые будут применены к виртуальному интерфейсу по мере необходимости.

виртуальный профиль: Экземпляр уникального интерфейса виртуального доступа, который создан динамично, когда некоторые пользователи призывают, и разъединен динамично, когда вызов разъединяет. Виртуальный профиль определенного пользователя может быть настроен интерфейсом виртуального шаблона, конфигурация интерфейса конкретного пользователя, сохраненная на AAA-сервере, или и интерфейс виртуального шаблона и конфигурация интерфейса конкретного пользователя от AAA.

Конфигурация интерфейса виртуального доступа начинается с интерфейса виртуального шаблона (если таковые имеются), придерживавшийся приложением конфигурации конкретного пользователя для сеанса наборного (телефонного) доступа индивидуального пользователя (если таковые имеются).

Аннотированный пример согласования PPP

В данном примере эхо-запрос переводит соединение ISDN в рабочее состояние между *Montecito* маршрутизаторов и *Goleta*. Обратите внимание на то, что, в то время как нет никакой установки штампов времени в данном примере, обычно рекомендуется использовать **service timestamps debug datetime msec** команды глобальной кофигурации.

Рисунок 16-12: МАРШРУТИЗАТОР ISDN МАРШРУТИЗАТОРА

Эти отладки взяты от *Montecito*; однако, отладка на *Goleta* выглядела бы почти такой же.

Примечание: Ваши отладки могут появиться в другом формате. Эти выходные данные являются более старым форматом вывода Отладки PPP, прежде чем модификации представили в версии IOS 11.2 (8). См. Главу 17 для примера Отладки PPP в более новых версиях IOS.

```
Montecito#show debugging PPP: PPP authentication debugging is on PPP protocol negotiation
debugging is on A Montecito#ping 172.16.20.2 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echoes to 172.16.20.2, timeout is 2 seconds: B %LINK-3-UPDOWN: Interface BRI0: B-Channel 1,
changed state to up C ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5 C ppp:
sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7 D PPP BRI0: B-Channel 1: received
config for type = 0x3 (AUTHTYPE) value = 0xC223 digest = 0x5 acked D PPP BRI0: B-Channel 1:
received config for type = 0x5 (MAGICNUMBER) value = 0x28FC9083 acked E PPP BRI0: B-Channel 1:
state = ACKsent fsm_rconfack(0xC021): rcvd id 0x65 F ppp: config ACK received, type = 3
(CI_AUTHTYPE), value = C223 F ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value =
29EBD1A7 G PPP BRI0: B-Channel 1: Send CHAP challenge id=1 to remote H PPP BRI0: B-Channel 1:
CHAP challenge from Goleta J PPP BRI0: B-Channel 1: CHAP response id=1 received from Goleta K
PPP BRI0: B-Channel 1: Send CHAP success id=1 to remote L PPP BRI0: B-Channel 1: remote passed
CHAP authentication. M PPP BRI0: B-Channel 1: Passed CHAP authentication with remote. N ipcp:
sending CONFREQ, type = 3 (CI_ADDRESS), Address = 172.16.20.1 P ppp BRI0: B-Channel 1: Negotiate
IP address: her address 172.16.20.2 (ACK) Q ppp: ipcp_reqci: returning CONFACK. R PPP BRI0: B-
Channel 1: state = ACKsent fsm_rconfack(0x8021): rcvd id 0x25 S ipcp: config ACK received, type
= 3 (CI_ADDRESS), Address = 172.16.20.1 T BRI0: install route to 172.16.20.2 U %LINEPROTO-5-
UPDOWN: Line protocol on Interface BRI0: B-Channel 1, changed state to up
```

A - Трафик генерируется для инициирования набираемой попытки.

B - Соединение установлено (отладки ISDN, не используемые в данном примере).

Начните LCP:

C - *Montecito* передает запросы конфигурации LCP за AUTHTYPE и за MAGICNUMBER.

D - *Goleta* передает свои CONFREQ. Если значение для MAGICNUMBER совпадает со значением, передаваемым *Montecito*, существует высокая вероятность, что циклично выполнена линия.

E - Это указывает, что *Montecito* передал подтверждения к CONFREQ *Goleta*.

F - *Montecito* получает CONFACK от *Goleta*.

Начните фазу проверки подлинности:

G, H - *Montecito* и *Goleta* бросают вызов друг другу для аутентификации.

J - *Goleta* отвечает на вызов.

K, L - *Goleta* успешно передает аутентификацию.

M - Сообщение от *Goleta* до *Montecito*: аутентификация выполнена успешно.

Согласование NCP начинается:

N, P - Каждый маршрутизатор передает свой настроенный IP - адрес в CONFREQ.

Q, R - *Montecito* передает CONFACK к CONFREQ *Goleta*.

S-? и наоборот.

T, U - Маршрут установлен от *Montecito* до *Goleta*, и протокол на интерфейсе изменяется на, указывая, что согласования NCP завершили успешно.

Прежде, чем вызвать специалистов центра технической помощи Cisco Systems

Прежде, чем вызвать Центр технической поддержки (TAC) Cisco Systems, удостоверьтесь, что вы прочитали эту главу и завершили действия, предложенные для проблемы вашей системы.

Кроме того, оформите результаты выполненных действий для предоставления более эффективной помощи:

Для всех проблем соберите выходные данные **show running config** и **show version**. Гарантируйте, что **service timestamps debug datetime msec** команды находится в конфигурации.

Для проблем DDR соберите придерживающееся:

- **show dialer map**
- **debug dialer –**
- **debug ppp negotiation –**
- **debug ppp authenticaion –**

Если ISDN включена, соберите:

- **show isdn status**
- **debug isdn q931**
- **debug isdn events**

Если модемы включены, собирают:

- выставочные подвиды

- выставочный подвид [x]
- **show modem** (если интегрированные модемы включены),
- **show modem version** (если интегрированные модемы включены),
- **debug modem –**
- **debug modem csm** (если интегрированные модемы включены),
- **отладьте чат** (если сценарий DDR)

Если T1s или PRI включены, собирают:

- **show controller t1**

Дополнительные сведения

- Руководство решений для коммутируемого доступа Cisco IOS
- Обзор интерфейсов, контроллеров и линий, используемых для коммутируемого доступа
- Маршрутизация через модемные линии
- Конфигурация последовательного порта и магистрали T1/E1
- Разработка объединений нескольких локальных сетей DDR
- Решение и подготовка настроить DDR
- Настройка DDRtitle
- Обзор технологии PPP
- Разработка объединений нескольких локальных сетей ISDN
- Типы коммутаторов ISDN, коды и значения
- Инициализация линии ISDN
- Cisco Systems – техническая поддержка и документация