

# Аппаратное и программное обеспечение ЭВМ и сетей

## Раздел 6 Технологии глобальных сетей

Тема 33-2 Протокол IP в глобальных сетях.

Чистая IP сеть. Протокол PPP.

Использование выделенных линий IP – маршрутизаторами. Работа IP-сети поверх сети ATM.

## Протокол IP в глобальных сетях. Чистая IP сеть.

- В настоящее время предоставлением транспортных услуг для распределенных- глобальных компьютерных сетей очень часто занимаются крупные провайдеры- операторы связи. Для предоставления качественных и разнообразных услуг большинство операторы связи применяют многоуровневую структуру технологий.
- Нижние уровни — это физические уровни- уровни первичной сети. К ним относятся технологии SDH/PDH, с пропускной способностью 2/1,5 -139,3/274,2Mb/s (для PDH) и 155,5Mb/s 10Gb/s(для SDH). На самом нижнем уровне первичной сети может работать наиболее скоростная на сегодняшний день технология DWDM, образующая спектральные каналы со скоростями 40 Гбит/с и выше.
- На основе первичной сети оператор сети может достаточно быстро организовать постоянный цифровой канал между точками подключения оборудования следующего уровня - наложенной сети — пакетной или телефонной.
- Следующим после двух физических уровней первичной сети может быть каналный уровень, основанный на технологиях ATM или FR, позволяющими использовать виртуальные каналы для продвижения кадров/ ячеек данных.
- Самый верхний уровень – это сетевой уровень, как правило построенный на технологии IP.
- Таким образом, получается четырех-уровневая структура современной глобальной сети - Рис. 6-33.1.

# Протокол IP в глобальных сетях. Чистая IP сеть.

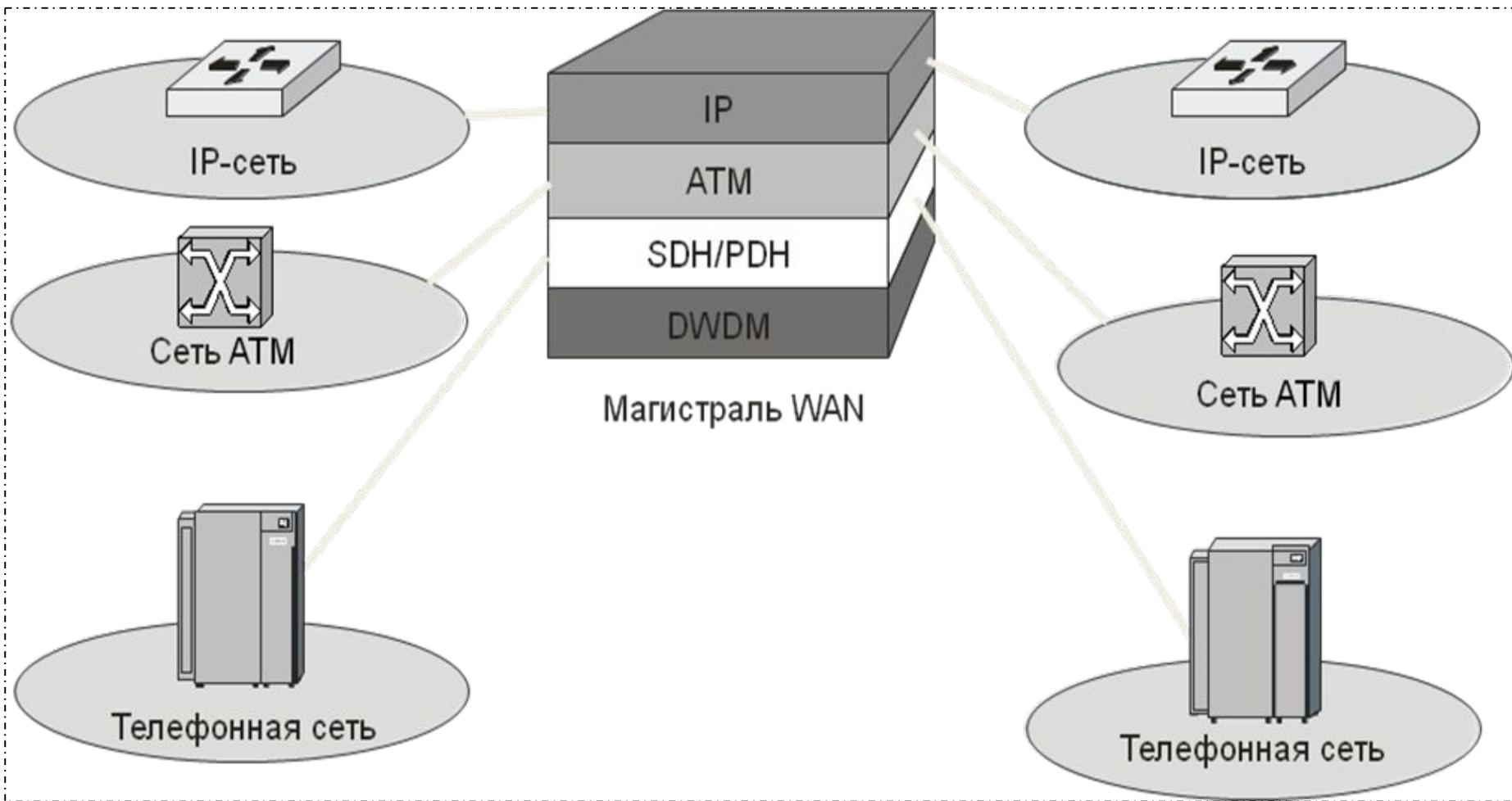


Рис. 6-33.1. Четырехуровневая структура современной глобальной сети

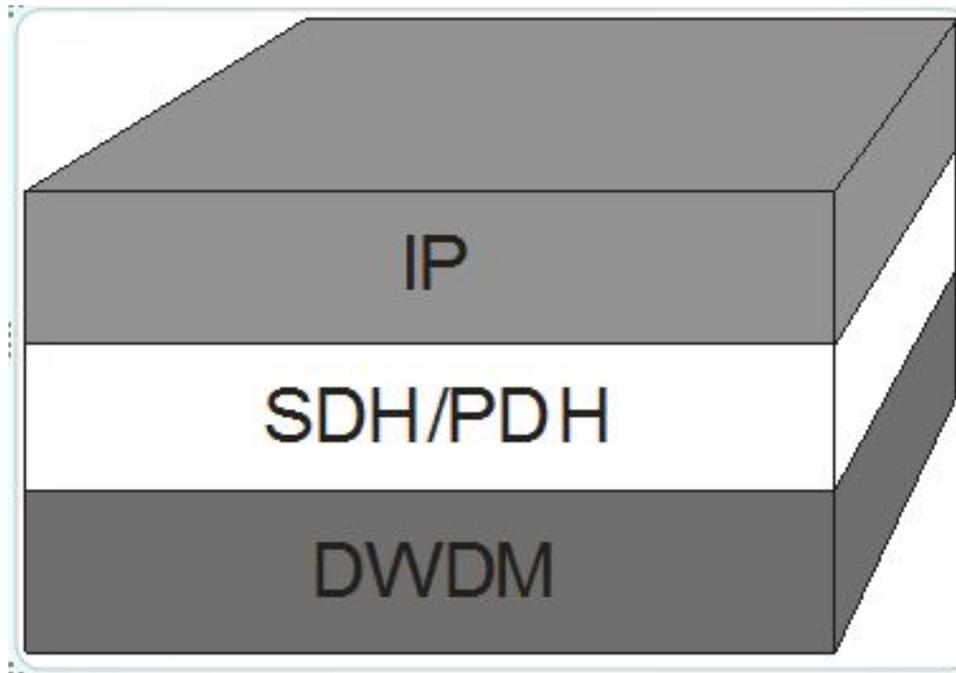
## Протокол IP в глобальных сетях. Чистая IP сеть.

- Во многих менее масштабных магистралях уровень DWDM отсутствует, технология SDH тоже применяется не всегда — вместо нее может работать менее скоростная и отказоустойчивая, но более экономичная технология PDH.
- Основным назначением уровня ATM на модели, изображенной на рис. 6-33.1, является создание инфраструктуры постоянных виртуальных каналов с гарантированным качеством обслуживания, соединяющих интерфейсы IP-маршрутизаторов. Для каждого класса IP-трафика в сети ATM образуется отдельный виртуальный канал, обеспечивающий требуемые для трафика параметры QoS — среднюю скорость, величину пульсаций, уровень задержек, уровень потерь. Применение ATM под уровнем IP позволяет не только обеспечить для пользовательского трафика необходимое качество обслуживания, но и дает возможность оператору решить задачу инжиниринга трафика предоставив сбалансированную загрузку всех линий связи первичной сети.
- Уровень IP, освобожденный в представленной модели от проблем обеспечения параметров QoS, выполняет свои классические функции — образует составную сеть и предоставляет IP-услуги конечным пользователям, передающим по глобальной сети свой IP-трафик транзитом или взаимодействующим по IP с Интернетом.

## Протокол IP в глобальных сетях. Чистая IP сеть.

- Первые IP-сети не имели такой сложной многослойной структуры. Классическая IP-сеть состояла из маршрутизаторов, непосредственно соединенных каналами связи. Эти сети не поддерживали QoS, так как трафик приложений 80-х годов не был чувствительным к задержкам. После появления многослойных глобальных IP-сетей возникла потребность различать эти два вида сетей, поэтому для классических IP-сетей мы будем использовать термин «чистая» IP-сеть.
- *«Чистая» IP-сеть отличается от многослойной тем, что под уровнем IP нет другой сети с коммутацией пакетов, такой как ATM или Frame Relay, и IP-маршрутизаторы связываются между собой выделенными каналами (физическими или соединениями PDH/SDH/DWDM).*
- В такой сети цифровые каналы по-прежнему образуются инфраструктурой двух нижних уровней, а этими каналами непосредственно пользуются интерфейсы IP-маршрутизаторов без какого-либо промежуточного уровня. В том случае, когда IP-маршрутизатор использует каналы, образованные в сети SDH/SONET, вариант IP-сети получил название пакетной сети, работающей поверх SONET (Packet Over SONET, POS).

# Протокол IP в глобальных сетях. Чистая IP сеть.



- **Рис. 6-33.2.** Структура «чистой» IP-сети
- «Чистая» IP-сеть может успешно применяться для передачи чувствительного к задержкам трафика современных приложений в двух случаях:
  - если IP-сеть работает в режиме низкой нагрузки, поэтому сервисы всех типов не страдают от эффекта очередей, так что сеть не требует применения методов поддержки параметров QoS;
  - если слой IP обеспечивает поддержку параметров QoS собственными средствами за счет применения механизмов IntServ или DiffServ.

# Протокол IP в глобальных сетях. Чистая IP сеть.

- Для того чтобы маршрутизаторы в модели «чистой» IP-сети могли использовать цифровые каналы, на этих каналах должен работать какой-либо протокол канального уровня. Существует несколько протоколов канального уровня, специально разработанных для двухточечных соединений глобальных сетей. В эти протоколы встроены процедуры, полезные при работе в глобальных сетях:
  - управление потоком данных;
  - взаимная аутентификация удаленных устройств, часто необходимая для защиты сети от «ложного» маршрутизатора, перехватывающего и перенаправляющего трафик для его прослушивания;
  - согласование параметров обмена данными на канальном и сетевом уровнях — при удаленном взаимодействии, когда два устройства расположены в разных городах, перед началом обмена часто необходимо автоматически согласовывать такие параметры, например, как MTU.
- Из набора существующих двухточечных протоколов протокол IP сегодня использует два: HDLC и PPP. Существует также устаревший протокол SLIP.
- Помимо уже упомянутых протоколов, в глобальных сетях на выделенных каналах IP-маршрутизаторы нередко используют какой-либо из высокоскоростных вариантов Ethernet: Fast Ethernet, Gigabit Ethernet или 10G Ethernet. Все варианты Ethernet не поддерживают перечисленных выше процедур, полезных для глобальных сетей, но чашу весов в данном случае перевешивает популярность этой технологии в локальных сетях.

# Протокол PPP

- Протокол PPP (Point-to-Point Protocol) является стандартным протоколом Интернета. Он предназначен для обмена данными на канальном уровне при соединении сетевых узлов по топологии «точка-точка», т.е. при непосредственном соединении узлов на физическом уровне. Предназначение PPP на канальном уровне:
  - 1) для непосредственного соединения удаленных хостов;
  - 2) пользователей услуг Интернет с портом маршрутизатора IPS;
  - 3) а также для непосредственного соединения маршрутизаторов между собой по топологии «точка-точка».

При разработке протокола PPP за основу был взят формат HDLC-кадров и дополнен несколькими полями, которые вложены в поле данных HDLC-кадра.

- Протокол PPP представляет собой целое семейство протоколов:
  - протокол управления линией связи (Link Control Protocol, LCP);
  - протокол управления сетью (Network Control Protocol, NCP);
  - многоканальный протокол PPP (Multi Link PPP, MLPPP);
  - протокол аутентификации по паролю (Password Authentication Protocol, PAP);
  - протокол аутентификации по квитированию вызова (Challenge Handshake Authentication Protocol, CHAP).

## Протокол PPP

- . Протокол поддерживает протоколы сетевого уровня такие как: IP – протокол, Novell IPX, AppleTalk, DECnet, XNS, Banyan VINES и OSI) достаточно универсален.

### Основные принципы работы

- Перед созданием канала с протоколом PPP в начале запускается пакет LCP(Link Control Protocol) для задания конфигурации соединения, а также проверки канала передачи данных. После того, как канал установлен и сконфигурирован LCP, иницилирующий протокол PPP отправляет пакеты NCP, чтобы выбрать и определить конфигурацию одного или более протоколов сетевого уровня. После выбора и конфигурации сетевого протокола, начинается продвижение дейтаграмм каждого протокола сетевого уровня. Канал сохраняет свою конфигурацию до тех пор, пока пакеты LCP или NCP явно не закроют его или пока не произойдет какое-нибудь внешнее событие (например, истечет срок бездействия таймера или вмешается какой-нибудь пользователь).

## Протокол PPP

### Требования, определяемые физическим уровнем

- PPP может работать через любой интерфейс DTE/DCE (например, EIA RS-232-C, EIA RS-422, EIA RS-423 и МСЭ-T V.35). Единственным абсолютным требованием, которое предъявляет PPP, является требование обеспечения физических схем (либо специально назначенных, либо переключаемых), которые могут работать как в синхронном, так и в асинхронном последовательном режиме, прозрачном для блоков данных канального уровня PPP. Протокол PPP не предъявляет каких-либо ограничений, касающихся скорости передачи информации, кроме тех, которые определяются используемым интерфейсом DTE/DCE.

# Протокол PPP

## □ Три составные части PPP:

□ Протокол содержит в себе три составные части:

- Метод инкапсуляции дейтограмм при передаче по последовательным коммуникационным каналам.
- Протокол LCP для установления, конфигурирования и тестирования информационных каналов
- Набор протоколов NCP для установки и конфигурирования различных протоколов сетевого уровня.

□ Протокол управления каналом (LCP - Link Control Protocol) является частью PPP.

## Протокол управления каналом LCP

□ Каждый кадр PPP начинается и завершается флагом 0x7E. За стартовым флагом-октетом следует байт адреса, который всегда равен 0xFF. Формат кадра PPP представлен на рис. 6-3305. Кадр PPP может содержать только целое число байт. При инкапсуляции других пакетов в PPP используется бит-ориентированный протокол HDLC (High-level Data Link Control).

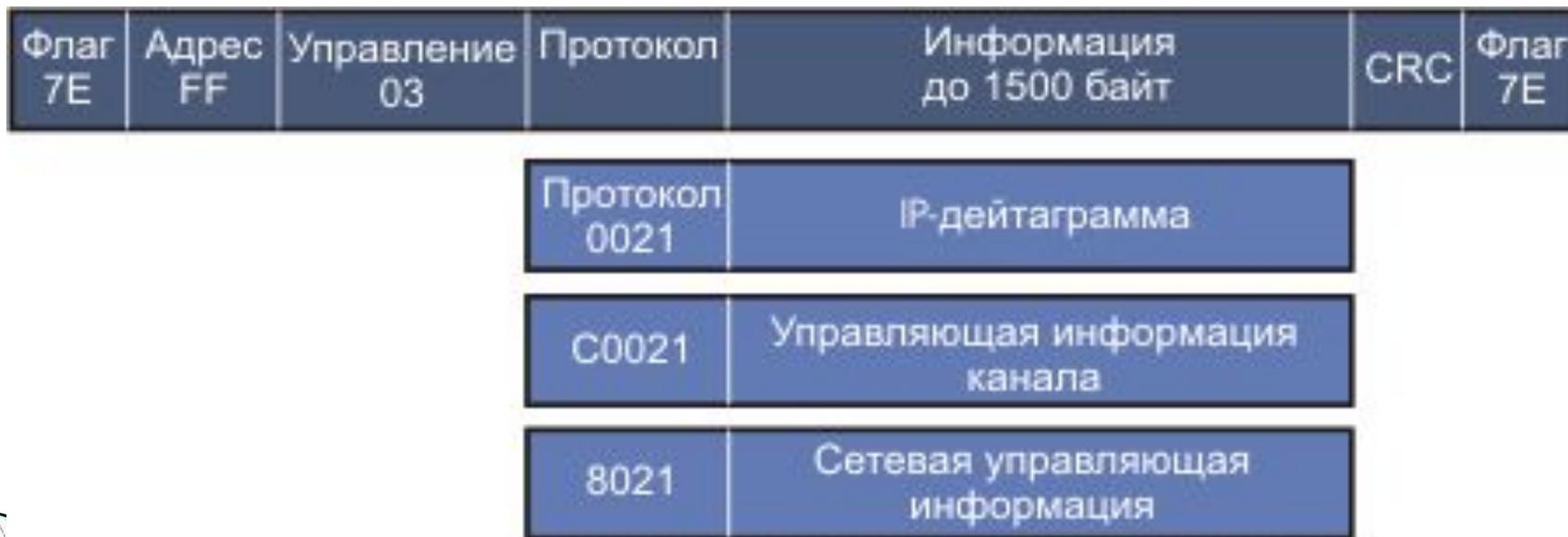
# Протокол PPP

## ▣ Существует три класса пакетов LCP:

- ▣ *Пакеты для организации канала связи.* Используются для организации и выбора конфигурации канала.
- ▣ *Пакеты для завершения действия канала.* Используются для завершения действия канала связи.
- ▣ *Пакеты для поддержания работоспособности канала.* Используются для поддержания и отладки канала.

▣ Рассмотрим формат кадра.

▣ Формат кадра представлен на рисунке ниже:



▣ Рис. 33.5. Формат кадра в протоколе PPP

## Протокол RPP

□ Процесс LCP проходит через четыре четко различаемые фазы:

□ **Организация канала и согласование его конфигурации.**

LCP сначала открывает связь (канал) и согласовывает параметры конфигурации. Эта фаза завершается после того, как будет отправлен и принят пакет подтверждения конфигурации.

□ **Определение качества канала связи.** LCP обеспечивает необязательную фазу определения качества канала, которая следует за фазой организации канала и согласования его конфигурации. В этой фазе проверяется канал с целью выяснения, является ли качество канала достаточным для вызова протоколов сетевого уровня. Эта фаза является полностью факультативной. LCP может задержать передачу информации протоколов сетевого уровня до завершения этой фазы.

## Протокол RRR

- ▣ **Согласование конфигурации протоколов сетевого уровня.** После того, как LSP завершит фазу определения качества канала связи, соответствующими NCP может быть выбрана конфигурация сетевых протоколов, и они могут быть в любой момент вызваны и освобождены для последующего использования. Если LSP закрывает данный канал, он информирует об этом протоколы сетевого уровня, чтобы они могли принять соответствующие меры.
- ▣ **Прекращение действия канала.** LSP может в любой момент закрыть канал. Это обычно делается по запросу пользователя, но может произойти также из-за какого-нибудь физического события, такого, как потеря носителя или истечение периода бездействия таймера.

# Протокол PPP

- **Поле адрес** всегда содержит байт 0xFF. Это указывает на то, что все станции должны принять этот кадр, и исключает необходимость выделения каких-то специальных адресов. Байт управления всегда равен 0x03, что указывает на ненумерованный тип кадра. По умолчанию кадры PPP передаются в режиме "без установления соединения". Если требуется надежная доставка, используется версия, описанная в RFC-1663.
- **Поле протокол** (двух октетное) сходно по функции с полем тип в кадре Ethernet и определяет то, как следует интерпретировать информационное поле (табл. 6-33.3). Значение 0x0021 этого поля говорит о том, что последующее информационное поле содержит в себе IP-дейтограмму.
- **Поле CRC** (Cyclic Redundancy Check) представляет собой циклическую контрольную сумму, предназначенную для выявления ошибок при транспортировке PPP-кадра.
- Применение **флагов-ограничителей кадра (0x7E)** создает проблему, - эти байты не могут присутствовать в информационном поле. В синхронном режиме эта проблема решается на аппаратном уровне. При работе в асинхронном режиме для этого используется специальный ESC-символ, равный 0x7D. Это необходимо делать, так как управляющие символы могут оказать непредсказуемые воздействия на режим работы драйверов или модемов, используемых в канале. Протокол PPP допускает мультипротокольность и динамическое определение IP-адресов партнеров.

Протокол PPP (Таблица 6-33.3

)

| Код протокола<br>(шестнадцатеричный) | Наименование протокола                             |
|--------------------------------------|--|
| 0001                                 | Протокол заполнения (padding)                      |
| 0003-001F                            | Зарезервировано                                    |
| <b>0021</b>                          | <b>IP-протокол</b>                                 |
| <b>0023</b>                          | <b>Сетевой уровень OSI</b>                         |
| <b>007D</b>                          | <b>Зарезервировано (Управление ESC - RFC 1661)</b> |
| <b>003F</b>                          | <b>Кадры NETBIOS</b>                               |
| <b>0029</b>                          | <b>Appletalk</b>                                   |
| <b>0041</b>                          | <b>Cisco System</b>                                |

# Протокол PPP

## □ Таблица 6-33.3 (продолжение)

|      |  |
|------|--|
| 0035 | <u>Banyan Vines</u>  |
| 0039 | <u>Appletalk EDDP</u>  |
| 003B | <u>Appletalk Smartbuffered</u>                               |
| 003D | <u>Multi-link</u>  |
| 003F | Кадры <u>Netbios</u>   |
| 0041 | <u>Cisco Systems</u>   |
| 0043 | <u>Ascom Timeplex</u>  |
| 0047 | Удаленная локальная сеть DCA                                 |
| 0049 | Транспортный протокол для последовательных данных (PPP-SDTP) |
| 004B | SNA через 802.2  |
| 004D | SNA  |
| 004F | Сжатие заголовков IPv6                                       |
| 007D | <u>Зарезервировано (Управл. ESC) [RFC1661]</u>               |
| 00FD | 1-ый вариант компрессии                                      |
| 0201 | Пакеты отклика 802.1d  |

# Протокол RRR

## □ Таблица 6-33.3 (продолжение)

|      |  |
|------|--|
| 0203 | IBM BPDU базовой маршрутизации             |
| 8021 | Управляющий протокол Интернет (IPCP)       |
| 8023 | Управляющий протокол сетевого уровня OSI   |
| 8025 | Управляющий протокол <u>Xerox NS IDP</u>   |
| 8027 | Управляющий протокол <u>Decnet фаза VI</u> |
| 8029 | Управляющий протокол <u>Appletalk</u>      |
| 802B | Управляющий протокол <u>Novell IPX</u>     |
| 8031 | Бридж NCP                                  |
| 8033 | Потоковый управляющий протокол             |
| 8035 | Управляющий протокол <u>Banyan Vines</u>   |
| 803D | Многосвязный управляющий протокол          |
| 803F | Управляющий протокол кадров <u>NetBIOS</u> |
| 8041 | Управляющий протокол <u>Cisco</u>          |

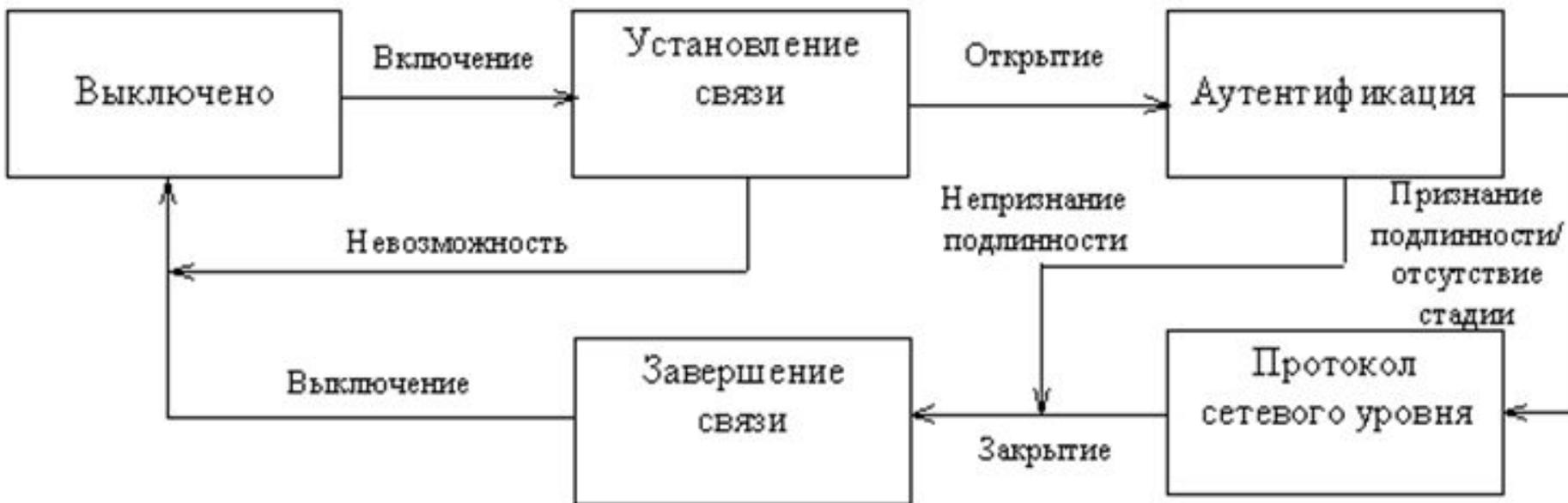
# Протокол PPP

## □ Таблица 6-33.3 (продолжение)

|      |  |
|------|--|
| 8043 | <u>Ascom</u> <u>Timeplex</u>                                     |
| 8045 | Управляющий протокол <u>Fujitsu</u> LBLB                         |
| 8047 | Управляющий протокол удаленных локальных сетей DCA (RLNCP)       |
| 8049 | Управляющий протокол передачи последовательных данных (PPP-SDCP) |
|      | Управляющий протокол для передачи <u>sna</u> поверх 802.2        |
| 804D | Управляющий протокол SNA   |
| 804F | Управляющий протокол сжатия заголовков IPv6                      |
| 80FD | Управляющий протокол сжатия                                      |
| C021 | Канальный управляющий протокол                                   |
| C023 | Протокол аутентификации паролей                                  |
| C025 | Сообщение о состоянии канала                                     |
| C081 | Управляющий протокол для работы с контейнерами                   |

## Протокол PPP

- Значения кодов поля протокола от 0xxx до 3xxx идентифицируют протоколы сетевого уровня, а значения в интервале 8xxx - Vxxx говорят о том, что протокол соответствует NCP (Network Control Protocol). Коды из диапазона 4xxx - 7xxx используются для протоколов с низким уровнем трафика, а коды от Sxxx до Exxx соответствуют управляющим протоколам (например, LCP).
- Протокол PPP при установлении соединения предусматривает процедуру аутентификации, которая является опционной (смотри рис. 6-33.6.). После перехода на сетевой уровень вызывается NCP-протокол, который выполняет необходимую конфигурацию канала.



□ Рис. 6-33.6. Алгоритм установления соединения PPP

# Протокол PPP

## Диаграмма стадий PPP

- При обнаружении несущей или по инициативе клиента система может попытаться установить соединение. В случае успеха система переходит в фазу аутентификации. Если же фаза аутентификации завершается благополучно, система выполняет подключение к сети (IP, IPX, Appletalk и т.д.), настройка сетевого уровня производится в рамках протокола NCP. Во всех остальных случаях производится возврат в исходное состояние. Процедура закрытия соединения осуществляется протоколом LCP.

### □ **Стадия "Выключено"**

- Связь обязательно начинается и заканчивается в стадии "Выключено" (физический уровень не готов). Когда внешнее событие (такое, как обнаружение носителя или конфигурация администратора сети) указывает, что физический уровень к использованию готов, PPP переходит к стадии "Установление связи".
- В течении этой стадии автомат LCP находится в состояниях "Начальное" или "Старт". Переход к стадии "Установление связи" выполняется по сигналу "Включение" автомату LCP.

### □ **Примечание:**

- Обычно, связь возвращается в эту стадию автоматически после разъединения модема. В случае интенсивной работы, эта стадия может быть чрезвычайно короткой - только для того, чтобы обнаружить присутствие устройства.

## Протокол RRP

### ▣ **Стадия "Установление связи"**

- ▣ Чтобы установить связь, протокол LSP обменивается пакетами выбора конфигурации. При завершении обмена LSP входит в состояние "Открыто" (когда пакет "Запрос конфигурации", был послан и получен).
- ▣ LSP конфигурируют только те опции конфигурации, которые являются независимыми от протоколов сетевого уровня. Конфигурация протоколов сетевого уровня выполняется в соответствии с отдельными протоколами контроля сети NCPs (на каждый тип сетевого протокола свой NCP) в течение стадии "Протокол сетевого уровня".
- ▣ Любые пакеты, не соответствующие протоколу LSP, полученные в течение этой стадии, должны быть отброшены без уведомления.
- ▣ Получение запроса конфигурации LSP вызывает переход из стадий "Протокол сетевого уровня" или "Аутентификация" к стадии "Установление связи".

## ▣ Стадия "Аутентификация"

- ▣ В некоторых случаях возникает необходимость подтверждения сетевым устройством своей подлинности.
- ▣ По умолчанию, установление подлинности не обязательно. Если приложение запрашивает использование протокола аутентификации, то эта процедура происходит в течение стадии "Установление связи".
- ▣ Переход от стадии "Аутентификация" к стадии "Протокол сетевого уровня" не должен наступать до завершения аутентификации. Если установление подлинности не выполнено, то должен произойти переход к стадии "Завершение связи".
- ▣ В течение данной стадии могут передаваться только пакеты протокола контроля связи LCP, протокола аутентификации и контроля качества связи. Приложение не должно завершать аутентификацию по тайм-ауту или при отсутствии ответа, и только после N-го количества попыток переходить к стадии "Завершение связи".
- ▣ Приложение, которое не признало подлинность сетевого объекта, инициирует стадию "Завершение связи".

## Протокол PPP

### ▣ **Стадия "Протокол сетевого уровня"**

- ▣ Когда PPP завершает предыдущие стадии, каждый протокол сетевого уровня (такой как IP, IPX или AppleTalk) должен быть индивидуально сконфигурирован согласно соответствующему протоколу контроля сети (NCP). Каждый NCP может быть открыт и закрыт в любое время.
- ▣ После того, как NCP достиг состояния "Открыто", PPP будет передавать соответствующие пакеты протокола сетевого уровня. Любые пакеты протокола сетевого уровня, полученные, когда NCP не находится в состоянии "Открыто", должны быть сброшены без уведомления.
- ▣ Примечание:
- ▣ Когда LCP находится в состоянии "Открыто", любой пакет протокола, который не поддерживается приложением, должен быть указан в пакете сброса протокола (Protocol-Reject), описанном ниже. Только пакеты поддерживаемых протоколов сбрасываются без уведомления.
- ▣ В течение этой стадии, трафик канала состоит из любой возможной комбинации пакетов LCP, NCP и протокола сетевого уровня.

# Протокол RRR

## ▣ **Стадия "Завершение связи"**

- ▣ RRR может расторгнуть связь в любое время. Это может случиться из-за потери носителя, непризнания подлинности при аутентификации, неудовлетворительного качества связи, истечения таймера незанятого периода или административного закрытия связи.
- ▣ LSR закрывает связь путем обмена пакетами разъединения. Когда связь закрывается, RRR информирует протоколы сетевого уровня.
- ▣ Отправитель запроса на разъединения разъединятся только после получения подтверждения разъединения или после того, как истечет счетчик перезапуска. Приемник запроса на разъединение ждет, пока сетевой объект не разъединится; он не должен разъединяться до тех пор, пока после подтверждения разъединения не пройдет по крайней мере один период перезапуска RRR и только тогда перейти к стадии "Выключено".
- ▣ Любой пакет не LSR, полученный в течение этой стадии, должен быть отброшен без уведомления.
- ▣ Закрытие канала связи с помощью LSR является достаточным. Посылать поток пакетов разъединения в каждом NCP нет необходимости. Более того, тот факт, что один NCP закрылся, не является достаточной причиной для разъединения канала RRR, даже если этот NCP был единственным в тот момент в состоянии "Открыто".

## Использование выделенных линий IP-маршрутизаторами

- Схема использования выделенной линии маршрутизатором показана на рис. 6-33.7.
- Для соединения порта маршрутизатора с выделенной линией необходимо использовать устройство DCE соответствующего типа. Это устройство требуется для согласования физического интерфейса маршрутизатора с интерфейсом физического уровня, используемого выделенной линией, например V.35.
- Если выделенная линия является аналоговой, то устройством DCE будет модем, а если цифровой — то аппаратура DSU/CSU.

# Использование выделенных линий IP-маршрутизаторами

**Аппаратура передачи данных** (АПД или *DCE - Data Circuit terminating Equipment*) в компьютерных сетях непосредственно присоединяет компьютеры или коммутаторы к линиям связи и является, таким образом, пограничным оборудованием. Традиционно аппаратуру передачи данных включают в состав линии связи. Примерами DCE являются модемы (для телефонных линий), терминальные адаптеры сетей ISDN, **устройства для подключения к цифровым каналам первичных сетей DSU/CSU (Data Service Unit /Circuit Service Unit).**

**Аппаратура пользователя линии связи,** вырабатывающая данные для передачи по линии связи и подключаемая непосредственно к аппаратуре передачи данных, обобщенно носит название **оконечное оборудование данных** (ООД или *DTE - Data Terminal*

# Использование выделенных линий IP-маршрутизаторами

Мост или маршрутизатор 1

Мост или маршрутизатор 2

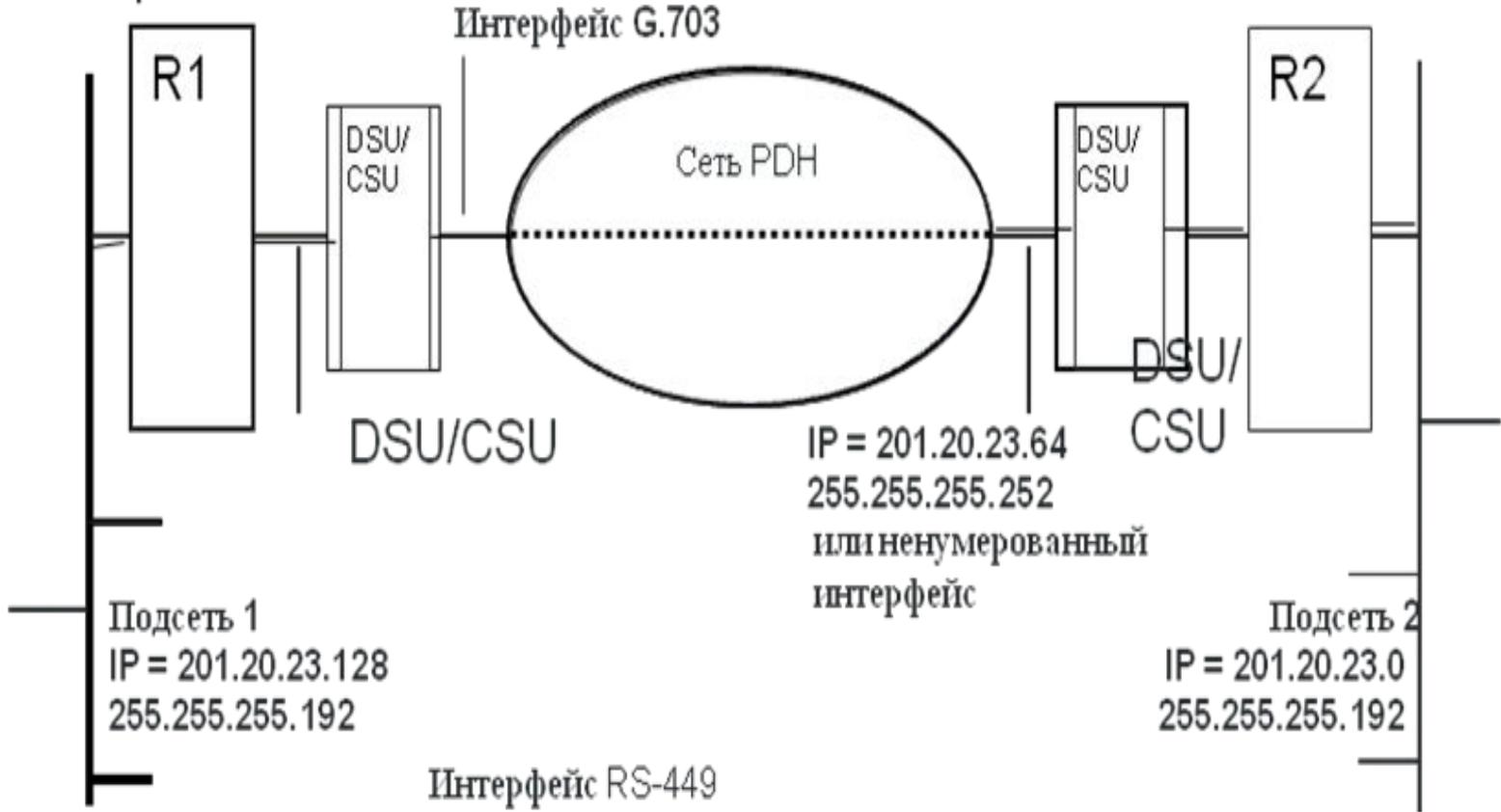


Рис. 6-33.7. Соединение IP-сетей с помощью выделенной линии

## Использование выделенных линий IP-маршрутизаторами

- Порт маршрутизатора может включать встроенное устройство DCE. Например, маршрутизатор, рассчитанный на работу с каналом SDH, обычно имеет встроенный порт с интерфейсом SDH определенной скорости STM-N.
- Встроенные порты PDH/SDH могут как поддерживать, так и не поддерживать внутреннюю структуру кадров этих технологий. В том случае, когда порт различает подкадры, из которых состоит кадр, например отдельные тайм-слоты кадра E1 или отдельные виртуальные контейнеры VC-12 (2 Мбит/с), входящие в кадр STM-1, и порт может использовать их как отдельные физические подканалы, то говорят, что это порт с разделением каналов. Каждому такому каналу присваивается отдельный IP-адрес. В противном случае порт целиком рассматривается как один физический канал с одним IP-адресом.
- В качестве примера на рис. 6-33.7 выбрано соединение двух маршрутизаторов через цифровой канал E1, установленный в сети PDH. Маршрутизатор использует для подключения к каналу устройство DSU/CSU с внутренним интерфейсом RS-449 и внешним интерфейсом G.703, который определен в качестве интерфейса доступа к каналам PDH.

## Использование выделенных линий IP-маршрутизаторами

- Маршрутизаторы после подключения к выделенной линии и локальной сети необходимо конфигурировать. Выделенный канал является отдельной IP-подсетью, как и локальные подсети 1 и 2, которые он соединяет. Этой подсети можно также дать некоторый IP-адрес из диапазона адресов, которым распоряжается администратор составной сети. В приведенном примере выделенному каналу присвоен адрес подсети 201.20.23.64, состоящей из 2-х узлов, что определяется маской 255.255.255.252.
- Интерфейсам маршрутизаторов, связанных выделенной линией, можно и не присваивать IP-адрес - такой интерфейс маршрутизатора называется ненумерованным. Действительно, отсылая пакеты протокола маршрутизации (RIP или OSPF) по выделенному каналу, маршрутизаторы непременно их получают. Протокол ARP на выделенном канале не используется, так как аппаратные адреса на выделенном канале не имеют практического смысла.

## Функционирование IP-сети поверх сети ATM/FR

- Ключевые слова: многослойная сеть IP/ATM, оверлейная (наложенная) сеть, QoS, виртуальный канал, топология виртуальных каналов, ATM-коммутаторы, логический интерфейс, подинтерфейс, конфигурирование интерфейса, классы трафика, протокол Q 2931.

### Взаимодействие слоев IP и ATM

- При построении IP-сети поверх сети ATM/FR между слоем каналов и слоем IP работает сеть ATM или Frame Relay (FR). Так как скорости, на которых работает сеть Frame Relay, как правило, не превышают 2 Мбит/с, а уровень задержек и их вариаций не входит в число параметров QoS, поддерживаемых данной технологией, то чаще всего в качестве промежуточного слоя магистрали применяется технология ATM.
- Взаимодействие слоя IP со слоем ATM иллюстрирует рис. 6-33.8.

# Функционирование IP-сети поверх сети ATM/FR

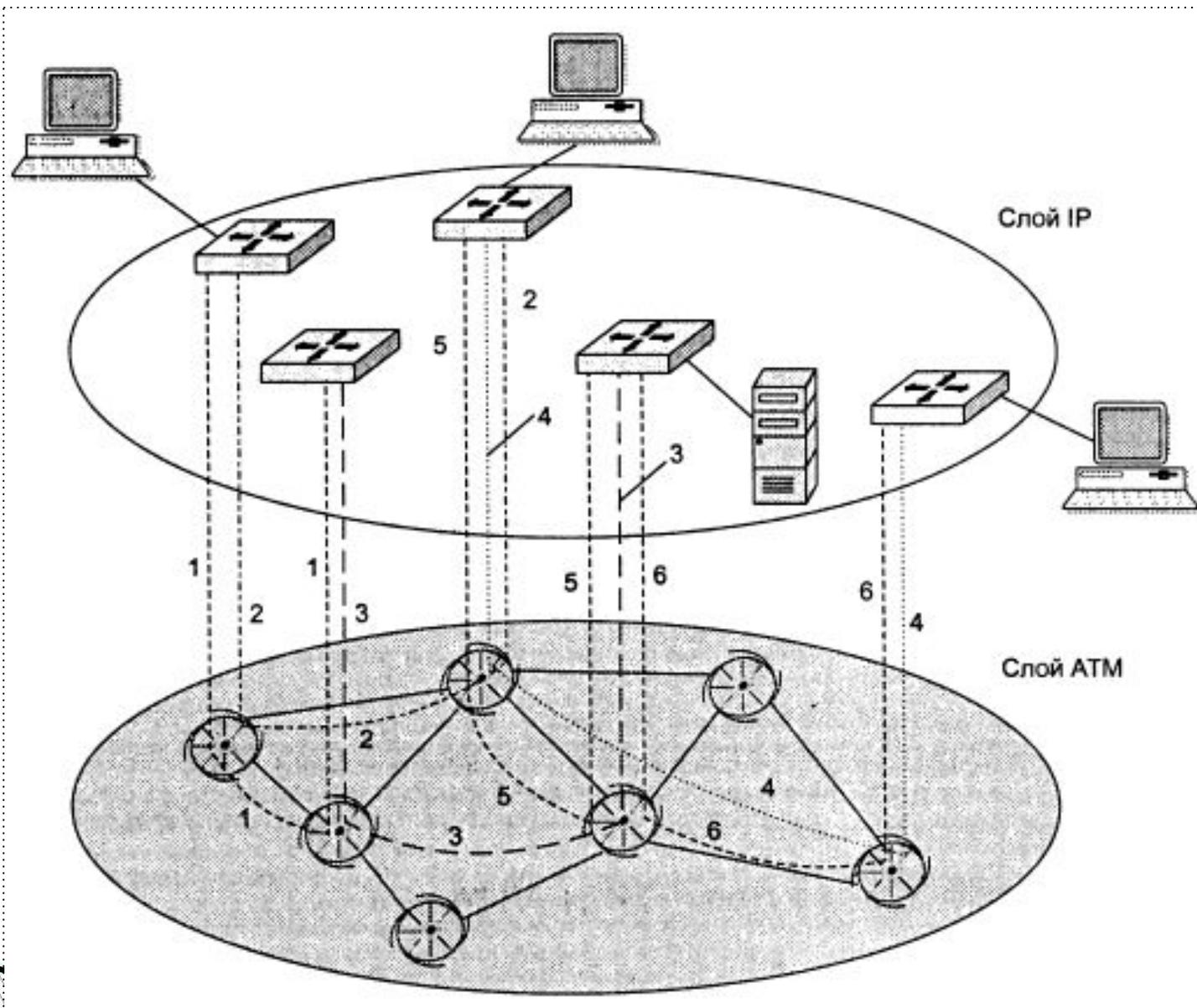
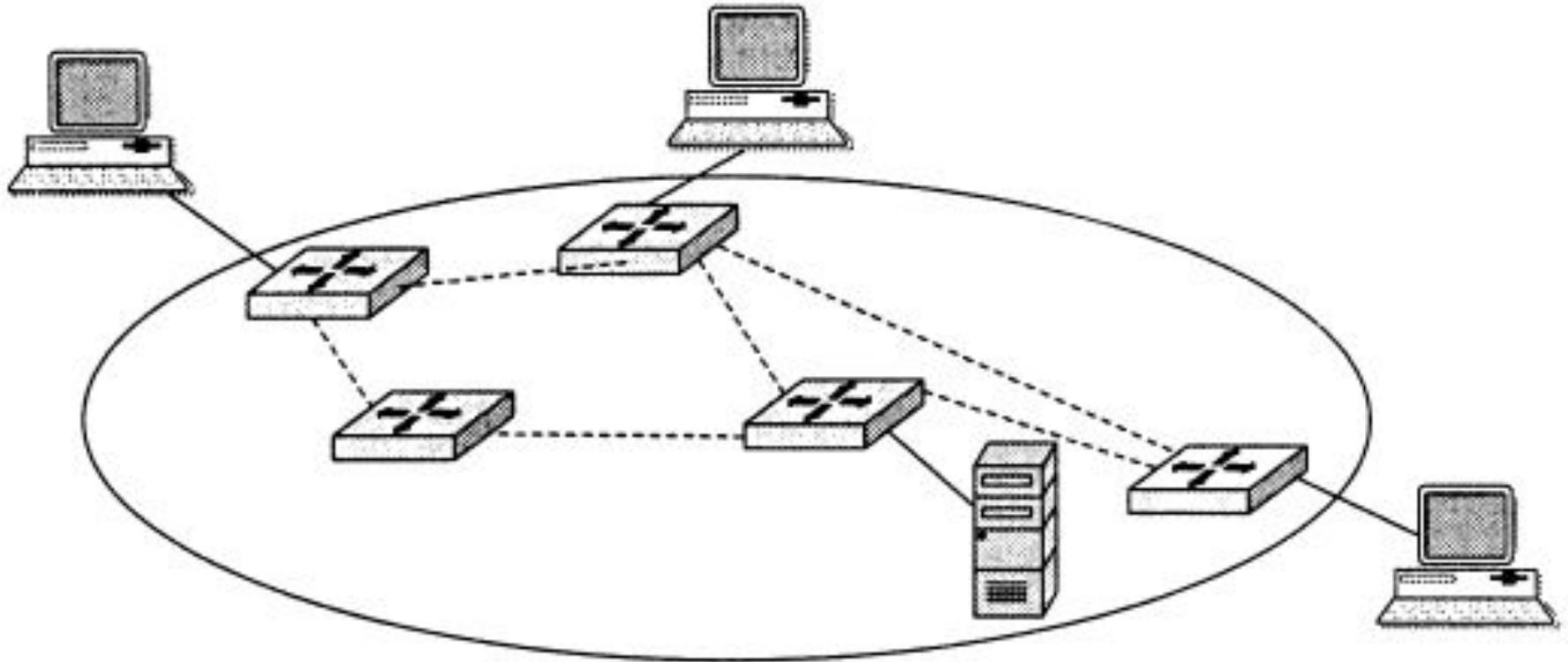


Рис. 6-33.8. Взаимодействие слоев IP и ATM

## Функционирование IP-сети поверх сети ATM/FR

- В сети ATM проложено шесть постоянных виртуальных каналов, соединяющих порты IP-маршрутизаторов. Каждый порт маршрутизатора должен поддерживать технологию ATM в качестве конечного узла. После того как виртуальные каналы установлены, маршрутизаторы могут пользоваться ими как физическими, посылая данные порту соседнего (по отношению к виртуальному каналу) маршрутизатора.
- В сети ATM образуется сеть виртуальных каналов с собственной топологией Топология виртуальных каналов, соответствующая сети, представленной на рис. 6-33.8, показана на рис. 6-33.9. Сеть ATM прозрачна для IP-маршрутизаторов, они ничего не знают о физических связях между портами ATM-коммутаторов, IP-сеть является наложенной (оверлейной) по отношению к сети ATM.

# Функционирование IP-сети поверх сети ATM/FR



□ Рис. 6-33.9. Топология связей между маршрутизаторами

# Функционирование IP-сети поверх сети ATM/FR

## Конфигурирование интерфейсов маршрутизаторов

- Для того чтобы протокол IP мог корректно работать, ему необходимо знать соответствие между IP-адресами соседей и адресами виртуальных каналов ATM, с помощью которых достигим соответствующий IP-адрес, то есть уметь отображать сетевые адреса на аппаратные, роль которых в данном случае играют адреса виртуальных каналов ATM. Другими словами, протоколу IP необходим некий вариант протокола ARP. Поскольку сеть ATM не поддерживает широковещательных запросов, таблица соответствия адресов не может быть создана автоматически. Администратор IP-сети должен вручную выполнить конфигурирование каждого интерфейса маршрутизатора, задав таблицу соответствия для всех номеров виртуальных каналов, исходящих и входящих в этот интерфейс. При этом физический интерфейс может быть представлен в виде набора логических интерфейсов (или подинтерфейсов), имеющих IP-адреса.
- Например, в маршрутизаторах компании Cisco Systems конфигурирование логического интерфейса, соответствующего виртуальному каналу с адресом VPI/VCI, равным 0/36, выглядит следующим образом:

```

pvc 0/36
  protocol ip 10.2.1.1

```

## Функционирование IP-сети поверх сети ATM/FR

- После выполнения этих команд маршрутизатор будет знать, что в случае необходимости пересылки пакета по адресу 10.2.1.1 ему нужно будет разбить пакет на последовательность ATM-ячеек (с помощью функции SAR интерфейса ATM) и отправить их все по постоянному виртуальному каналу с адресом 0/36.
- Если многослойная сеть IP/ATM должна передавать трафик различных классов с соблюдением параметров QoS для каждого класса, то соседние маршрутизаторы должны быть связаны несколькими виртуальными каналами, по одному для каждого класса. Маршрутизатору должна быть задана политика классификации пакетов, позволяющая отнести передаваемый пакет к определенному классу. Пакеты каждого класса направляются на соответствующий виртуальный канал, который обеспечивает трафику требуемые параметры QoS. Однако предварительно необходимо провести инжиниринг трафика для сети ATM, определив оптимальные пути прохождения трафика и соответствующим образом проложив виртуальные каналы. Результатом такой работы будет соблюдение требований к средним скоростям потоков, а коэффициент загрузки каждого интерфейса ATM- коммутаторов не превысит определенной пороговой величины, гарантирующей каждому классу трафика приемлемый уровень задержек.

## Функционирование IP-сети поверх сети ATM/FR

- Оверлейная IP-сеть может также использовать режим коммутируемых виртуальных каналов (SVC) для передачи IP-трафика. Этот режим подходит для неустойчивых потоков, которые существуют в течение небольших периодов времени. Создавать для таких потоков инфраструктуру постоянных виртуальных каналов невыгодно, так как большую часть времени они будут простаивать. Для того чтобы маршрутизаторы могли использовать режим SVC, необходимо задать отображение IP-адресов, но не на номера виртуальных каналов, а на ATM-адреса конечных точек сети ATM, то есть ATM-адреса интерфейсов маршрутизатора.
- Эта функция разрешения адресов, как и в предыдущем случае, выполняется администратором вручную. Один из вариантов задания такого отображения для маршрутизаторов Cisco имеет следующий вид:

**Map-list a**

**ip 10.1.0.3 atm-nsap**

**33.3333.33.3333.00.3333.3333.3333.3333.3333.3333.33**

## Функционирование IP-сети поверх сети ATM/FR

- Если задано такое соответствие адресов, маршрутизатор для отправки пакета по IP-адресу 10.1.0.3 предварительно устанавливает с помощью протокола Q.2931 коммутируемый виртуальный канал SVC с ATM-адресом 33.3333.33.333333.3333.3333.333333333.3333.3333.3333.33, а затем, автоматически получив от этого протокола адрес VPI/VCI, отправляет по нему ячейки, на которые разбит исходный пакет. Интерфейс соседнего маршрутизатора, получив все ячейки, объединяет их в исходный пакет и передает наверх протоколу IP.
- Если по коммутируемому виртуальному каналу нужно передавать трафик с некоторыми требуемыми параметрами QoS, то эти параметры передаются протоколу Q.2931, который выбирает маршрут для виртуального канала с их учетом.
- Функционирование IP-сети поверх сети ATM очень популярно у операторов связи, которые предоставляют услуги с заключением соглашения об уровне обслуживания (SLA).

## **Список использованных источников**

- В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г.