**ПЛАН ЗАНЯТИЯ № 4**

**Тема 1.4 «Стандартизация работы сети»**

**ЦЕЛИ:**

**Образовательные:**

* Сформировать у учащихся представление о протоколах TCP и UDP.
* Сформировать у учащихся представление о протоколах прикладного уровня.
* Сформировать у учащихся представление о портах TCP/IP и их номерах.
* Сформировать у учащихся представление о модели TCP/IP.
* Сформировать у учащихся представление о структура пакета.

**Развивающие:**

* Способствовать дальнейшему формированию знаний и умений у учащихся по изучаемой дисциплине.
* Развитие логических умений при изучении модели TCP/IP.
* Развитие навыков конспектирования материалов.

**Воспитательные:**

* Развитие познавательного интереса.

**Вид занятия** – лекция

**Тип** (урок) – комбинированный урок

**Методы –** словесные, наглядные

**Средства обучения** – презентация, проектор, ПК

**ХОД ЗАНЯТИЯ**

1. **Организационный момент**
   * Приветствие.
   * Проверка явки
2. **Целеполагание**

* Цели (задачи), ход занятия.

1. **Актуализация знаний**

**Фронтальный опрос по следующим вопросам**

1. Устройство коаксиального кабеля.

2. Тонкий коаксиальный кабель. Его характеристики.

3. Толстый коаксиальный кабель. Его характеристики.

4. Устройство кабеля типа витая пара.

5. Неэкранированная витая пара. Категория 1, категория 2.

6. Неэкранированная витая пара. Категория 3, категория 4.

7. Неэкранированная витая пара. Категория 5, категория 5е.

8. Неэкранированная витая пара. Категория 6, категория 6а, категория 7.

9. Экранированная витая пара. Type 1 и Type 2.

10. Беспроводная связь.

11. Полнодуплексная и полудуплексная передача.

**Изучение нового**

* Знать отличия протоколов TCP и UDP.
* Знать модель TCP/IP. Принципы ее работы.
* Знать структуру пакета
* Знать беспроводные каналы и их характеристики
* Знать характеристики процесса передачи

1. **Закрепление изученного**

* Для закрепления полученных знаний проводится беседа по основным понятиям и определениям рассмотренной темы

- Принцип работы протокола TCP.

- Принцип работы протокола UDP.

- Протоколы модели TCP/IP.

- Основные порты модели TCP/IP и их номера.

1. **Домашнее задание**

* Опорный конспект.
* Ответы на контрольные вопросы.

1. **Выставление оценок с комментариями**

**Теоретический материал**

Работа сети заключается в передаче данных от одного ПК к другому. В этом процессе можно выделить несколько отдельных задач:

* распознать данные;
* разбить данные на управляемые блоки;
* добавить информацию к каждому блоку, чтобы:

- указать местонахождение данных;

- указать получателя;

* добавить информацию для проверки ошибок;
* поместить данные в сеть и отправить по заданному адресу.

Сетевая операционная система при выполнении всех задач следует строгому набору процедур. Эти процедуры называются протоколами или правилами поведения. Протоколы регламентируют каж­дую операцию. Протокол – это система правил, которые позволяют всем компьютерам, знающим эти правила, общаться друг с другом.

Стандартные протоколы позволяют программному и аппаратному обеспечению различных производителей нормально взаимодействовать. Существуют два главных набора стандартов: модель OSI и ее модификация, называемая Project 802.

**Эталонная модель взаимодействия открытых систем**

Эталонная модель взаимодействия открытых систем (модель OSI) – это коммуникационная структура, разработанная Международной организацией по стандартизации (ISO). Первый набор спецификаций был выпущен в 1918 г. Международным стандартом стала версия 1984 г. Эталонная модель OSI очень важна для сетевой индустрии, поскольку производители сетевых продуктов стремятся к совместимости своих продуктов с продуктами других поставщиков. Модель OSI предоставляет независимым производителям общий набор критериев, которых они должны придерживаться при разработке своих продуктов.

Что же касается набора протоколов, то официально реализация каждого уровня модели OSI в качестве стандарта продолжается уже много лет, при этом было выпущено всего несколько коммерческих версий.

**Многоуровневая архитектура**

Эталонная модель взаимодействия открытых систем (OSI) описывает семь уровней взаимодействия между сетевыми устройствами. Эти уровни пронумерованы последовательно, начиная с реальных физических аппаратных соединений (уровень 1) и заканчивая уровнем обслуживания приложений или других программ, которые работают в сети (уровень 7). Каждый уровень взаимодействует только со смежным уровнем. Эта модель представлена в таблице.

Семь уровней модели OSI

**Уровень Клиент Сервер**

**7 Приложений «---виртуальная связь---» Приложений**

**6 Представлений «---виртуальная связь---» Представлений**

**5 Сеансовый «---виртуальная связь---» Сеансовый**

**4 Транспортный «---виртуальная связь---» Транспортный**

**3 Сетевой «---виртуальная связь---» Сетевой**

**2 Канальный «---виртуальная связь---» Канальный**

**1 Физический «---виртуальная связь---» Физический**

Таблица 1. Уровни эталонной модели взаимодействия открытых систем

Два нижних уровня определяют физическую среду передачи данных и сопутствующие задачи. Самые верхние уровни определяют, каким способом осуществляется доступ приложений к услугам связи. Чем выше уровень, тем более сложную задачу он решает. Уровни отделяются друг от друга границами – интерфейсами. Все запросы от одного уровня к другому передаются через интерфейс. Задача каждого уровня – предоставление услуг вышестоящему уровню. Интерфейс определяет эти услуги и способ доступа к ним. При этом каждый уровень на одном ПК работает так, будто он напрямую связан с таким же уровнем на другом ПК. Однако в действительности связь осуществляется между смежными уровнями одного ПК – ПО, работающее на каждом уровне, реализует определенные сетевые функции в соответствии с набором протоколов. Перед подачей в сеть данные разбиваются на пакеты. Пакет – это единица информации, передаваемая между устройствами сети как единое целое.

Пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется некая информация, которая необходима для передачи по сети.

На принимающей стороне пакет проходит все уровни в обратном порядке. Программное обеспечение на каждом уровне читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до прикладного уровня, вся адресная информация будет удалена и данные примут свой первоначальный вид.

Таким образом, никакой уровень, за исключением самого нижнего уровня сетевой модели, не может непосредственно послать информацию соответствующему уровню другого ПК. Информация на ПК-отправителе должна пройти через все уровни. Затем она передается по сетевому кабелю на компьютер-получатель и опять проходит через все слои, пока не достигнет того уровня, с которого она была послана. Не всем типам данных необходимо проходить все уровни – некоторые данные в определенной модели ничего не значат. Соответствующая модели OSI схема «получатель-отправитель» приведена на рисунке 2.2. В процессе передачи каждый уровень «дополняет» данные и заголовок предыдущих уровней своим собственным заголовком. Небольшой кадр данных постепенно обрастает заголовками всех уровней, которые он проходит. На стороне получателя все наоборот – каждый уровень будет «отсекать» соответствующий заголовок. Рисунок 2.3 иллюстрирует способ дополнения данных уровнями OSI.

Модель OSI следует использовать в качестве наглядного представления способа передачи данных в сети. Необходимо учитывать, что путь прохождения данных показан с изрядной долей абстракции.

• Уровень 1 (физический) о**пределяет физическую среду, используемую для передачи данных по локальной сети. На этом уровне описываются физические среды** (например, волоконно оптический кабель, витая пара и коаксиальный кабель), используемые для соединения между собой различных компонентов сети. **Физический уровень осуществляет передачу неструктурированного потока битов по физической среде от одного ПК к другому**. Здесь реализуются электрический, оптический, механический и функцио¬нальные интерфейсы с кабелем. Физический уровень также **формирует сигналы, которые переносят данные, поступающие от всех вышестоящих уровней**. **На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера**, в частности, количество контактов и разъемов и их функции. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что переданная единица будет воспринята как единица, а не как нуль. Наконец, **Физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы**;

• Уровень 2 (канальный) осуществляет передачу кадров (frames) данных от Сетевого уровня к Физическому. Кадры – это логически организованная структура, в которую можно помещать данные. Идентификаторы – это адреса ПК отправителя и получателя. Управляющая информация используется для маршрутизации, а также указывает на тип пакета и сегментацию. CRC – это сведения для выявления ошибок. Канальный уровень обеспечивает точность передачи кадров между ПК через Физический уровень. Это позволяет Сетевому уровню считать передачу данных по сетевому соединению практически безошибочной. На этом уровне определяются методы получения доступа к сети и передачи пакетов данных от одного устройства к другому (например, с помощью маркеров и кодов обнаружения ошибок). На этом уровне выполняется повторная передача пакетов данных, которые не дошли до пункта назначения. На этом уровне обеспечивается работа платы сетевого адаптера;

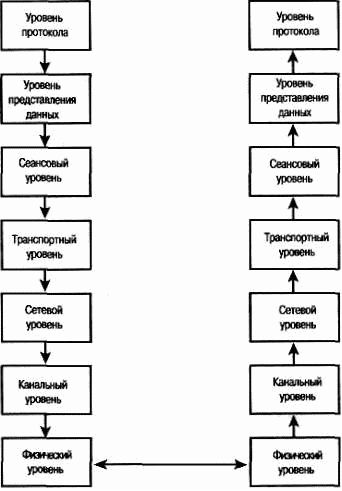


Рис. 2.2. Пример приема/передачи данных в модели OSI

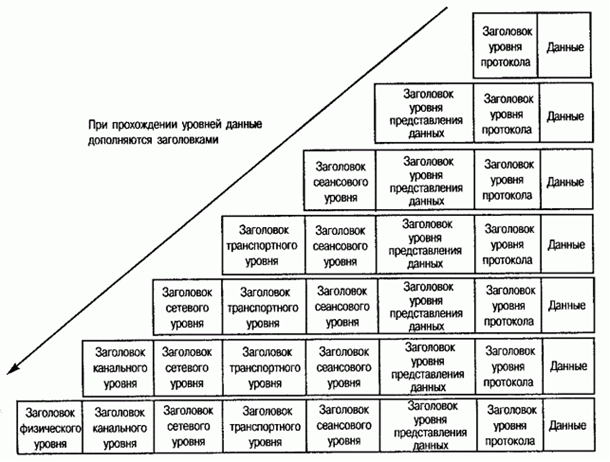


Рис. 2.3. Дополнение данных заголовками в модели OSI

• Уровень 3 (сетевой) отвечает за поиск рабочей станции, которой адресованы данные. Здесь происходит адресация сообщений, перевод логических имен и адресов в физические адреса. Исходя из конкретных сетевых условий, здесь определяется маршрут от отправителя к получателю. Если данные могут передаваться в локальной сети по нескольким маршрутам, то именно на сетевом уровне должен быть выбран лучший из них. На этом уровне решаются также проблемы, связанные с сетевым трафиком, такие как коммутация пакетов, маршрутизация и перегрузка. Если сетевой адаптер маршрутизатора не может передавать большие блоки данных, посланные отправителем на Сетевом уровне, эти блоки разбиваются на меньшие. Сетевой уровень получателя собирает эти данные в исходное состояние. Уровень 3 – наивысший из тех, на которых учи-тывается физическая конфигурация сети;

• Уровень 4 (транспортный) обеспечивает надежную транспортировку данных. Этот уровень отвечает за преобразование сообщений в форматы, требуемые для передачи по сети. На этом уровне сообщения переупаковываются: длинные разбиваются на несколько пакетов, а короткие объединяются в один. Это увеличивает эффективность передачи. На Транспортном уровне получателя сообщения распаковываются и восстанавливаются в первоначальном виде, и обычно посылается сигнал подтверждения приема. Если передача не выполнена, транспортный уровень регламентирует повторную передачу. Транспортный уровень управляет потоком, проверяет ошибки и участвует в решении проблем, связанных с отправкой и получением пакетов;

• Уровень 5 (сеансовый) описывает процедуру установления соединения для того, чтобы одно приложение (или пользователь) могло взаимодействовать с другим приложением на удаленном компьютере. Это соединение называется сеансом. На этом уровне происходит распознавание имен и защита, необходимые для связи двух приложений в сети. На этом уровне регламентируются также постановка в очередь поступающих сообщений, разрыв соединения и восстановление после аварийного завершения. Сеансовый уровень обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных контрольных точек. Таким образом, в случае ошибки заново потребуется передать только данные, следующие за контрольной точкой;

• Уровень 6 (представления) отвечает за то, чтобы команды и данные приложений были понятны на других компьютерах сети. Другими словами, на этом уровне происходит преобразование данных из одних форматов в другие, кроме того, этот уровень определяет механизмы шифрования и сжатия данных;

• Уровень 7 (приложений) описывает взаимодействие с прикладными процессами. Он представляет собой окно для доступа прикладных процессов к сетевым услугам. На этом уровне регламентируются сообщения, которые приложения должны использовать для запроса друг у друга данных и услуг. Этот уровень отвечает за предоставление услуг по распределенной обработке, включая обработку файлов, обработку ошибок, управление базами данных и управление сетью.

**Модель IEEE Project 802**

Основной международной организацией, устанавливающей коммуникаци­онные стандарты, является *Институт инженеров по электротехнике и элек­тронике* (Institute of Electrical and Electronics Engineers, IEEE). IEEE — сооб­щество профессионалов, объединяющее научные, технические и образова­тельные учреждения в более чем 150 странах. Входящий в IEEE Комитет по локальным сетям Компьютерного общества (Computer Society Local Network Committee) разработал многие из используемых в настоящее время сетевых стандартов. Одними из важнейших являются стандарты 802, определяющие характеристики физических кабелей и методы передачи данных в локальных сетях. Разработка стандартов 802 началась в феврале 1980 г. с создания комитета IEEE 802 и Проекта 802.

В Институт инженеров по электротехнике и электронике (IEEE, Institute for Electri­cal and Electronic Engineers) реализовал проект под названием Project 802, помогающий определить некоторые стандарты локальных сетей.

Хотя публикация стандартов IEEE опередила публикацию стандартов ISO, оба проекта велись приблизительно в одно время и при полном обмене информацией, что привело к появлению двух совместимых моделей.

Проект 802 определяет различные аспекты сети, относящиеся к физической кабельной системе и передаче данных, что соответствует физическому и канальному уровням модели OSI. Специфика­ции 802 предусматривают 12 категорий:

802.1 – Межсетевое взаимодействие;

802.2 – Управление логической связью (LLC, Logical Link Control);

802.3 – Множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD, Carrier Sense with Multiple Access and Collision Detection).(Ethernet);

802.4 – ЛВС с топологией «шина» с передачей маркера (Token Bus);

802.5 – ЛВС с топологией «кольцо» с передачей маркера (Token Ring);

802.6 – Средние и городские сети (MAN, Metropolitan Area Network);

802.7 – Консультативный совет по широковещательной технологии;

802.8 – Консультативный совет по оптоволоконной технологии;

802.9 – Сети для совместной передачи речи и данных;

802.10 – Защита в сетях;

802.11 – Беспроводные сети;

802.12 – ЛВС с доступом по приоритету запроса (Demand Priory Access LAN, 100BaseVG‑AnyLan).

- 802.14: стандарты на коммуникации с использованием широкополосного телевизионного кабеля;

- 802.15: стандарты на персональные сети, использующие беспроводные коммуникации;

- 802.16: стандарты на региональные сети, использующие широкополосные беспровод

Два нижних уровня модели OSI (Физический и Канальный) устанавливают, каким образом не­сколько ПК могут одновременно использовать сеть, не мешая друг другу. IEEE Project 802 отно­сится именно к этим уровням. Согласно этим спецификациям, Канальный уровень был разбит на два подуровня:

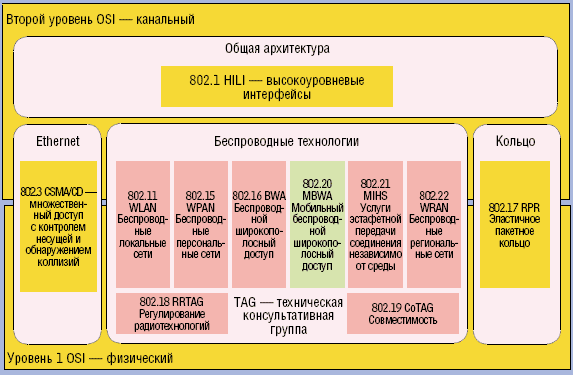
- ***Подуровень управления логической связью*** (**LLC, Logical Link Control**), обеспечивающий кон­троль ошибок и управление потоком передачи данных. Он устанавливает канал связи и определяет использование логических точек интерфейса, называемых точками доступа к услугам (SAP, Service Access Point). Другие ПК, ссылаясь на точки доступа к услугам, могут передавать информацию с подуровня Управления логической связью на верхние уровни модели OSI;

- ***Подуровень управления доступом к среде*** (**MAC, Media Access Control**), реализующий контроль доступа. Нижний из двух подуровней. Он обеспечивает совместный доступ плат сетевого адаптера. Этот подуровень напрямую связан с платой сетевого адаптера и отвечает за безошибочную пере­дачу данных между двумя ПК.

**Обзор актуальных стандартов IEEE 802 за последние время**

Проектная группа IEEE P802 — комитет по стандартам для локальных и городских сетей (LAN & MAN Standards Committee, LMSC) — разрабатывает стандарты, не связанные с IP. Два коллектива разработчиков, входящие в ее состав, занимаются очень важными направлениями — Ethernet и радиотехнологиями, соответственно. Тематика мобильной связи относится к юрисдикции рабочих групп, выделенных на Рисунке 1 красным цветом:

* 802.11 — беспроводные локальные сети (Wireless Local Area Networks, WLAN);
* 802.15 — беспроводные персональные сети (Wireless Personal Area Networks, WPAN);
* 802.16 — широкополосный беспроводной доступ (Broadband Wireless Access, BWA);
* 802.18 — техническая консультативная группа по регулированию радиотехнологий (Radio Regulatory Technical Advisory Group, RRTAG);
* 802.19 — техническая консультативная группа по совместимости (Coexistence Technical Advisory Group, CoTAG);
* 802.21 — услуги эстафетной передачи соединения независимо от среды (Media Independent Handover Services, MIHS);
* 802.22 — беспроводные региональные сети (Wireless Regional Area Networks, WRAN).



Рабочая группа 802.3 изучает проблемы Ethernet и занимается множественным доступом с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection, CSMA/CD). Как и прежде, ей принадлежит решающая роль в решении задач, нацеленных на увеличение пропускной способности. Большой активностью отличается и рабочая группа 802.1 HILI, деятельность которой посвящена высокоуровневым интерфейсам (HIgher Layer Interfaces, HILI) и направлена на удовлетворение потребностей провайдеров; таким образом, она выходит за рамки локальных и городских сетей.

**Функции пакетов**

Данные обычно содержатся в больших файлах. Но сеть не будет нормально рабо­тать, если компьютер посылает блок данных целиком. Существуют две причины, замедляющие работу сети при передаче по кабелю больших блоков данных. Во-первых, такой блок, посылаемый одним компьютером, заполняет кабель и «связывает» работу всей сети, т. е. препятствует взаимодействию остальных сетевых компонентов. Во-вторых, возникновение ошибок при передаче круп­ных блоков приведет к повторной передаче всего блока. А если поврежден небольшой блок дан­ных, то требуется повторная передача только этого блока, что значительно экономит время.

Чтобы быстро и легко, не тратя времени на ожидания, передавать по сети данные, надо разбить их на небольшие упорядоченные блоки. Эти блоки называются пакетами или кадрами. Хотя термины «пакет» и «кадр» синонимичны, полными синонимами они все-таки не являются. Существуют раз­личия между типами сети, которые эти термины отражают.

**Примечание**

*Среди специалистов по сетям существует разногласие по поводу точных опре­делений терминов «пакет» и «фрейм». Некоторые не делают различия между этими понятиями, однако многие специалисты соглашаются с тем, что фреймы представляют информацию, используемую на Уровне 2 модели OSI, а пакеты относятся к Уровню 3 модели OSI.*

***Пакет*** **–** основная единица информации в компьютерных сетях. При разбиении данных на пакеты скорость их передачи возрастает настолько, что каждый компьютер в сети получает возможность принимать и передавать данные практически одновременно с остальными компьютерами. На целе­вом компьютере (компьютере-получателе) пакеты накапливаются и выстраиваются в должном по­рядке для восстановления исходного вида данных.

При разбиении данных на пакеты сетевая операционная система добавляет к каждому пакету специ­альную управляющую информацию. Она обеспечивает:

* передачу исходных данных небольшими блоками;
* сбор данных в надлежащем порядке (при их получении);
* проверку данных на наличие ошибок (после сборки).

**Структура пакета**

Пакеты могут содержать несколько типов данных:

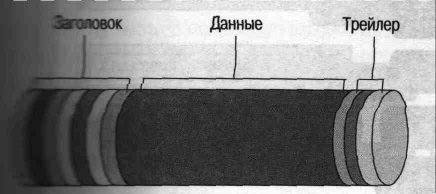
* информацию (например, сообщения или файлы);
* определенные виды данных и команд, управляющих компьютером (например, запро­сы к служ­бам);
* коды управления сеансом (например, запрос на повторную передачу для исправления ошибки).

**Основные компоненты**

Некоторые компоненты являются обязательными для всех типов пакетов:

* адрес источника (source), идентифицирующий компьютер-отправитель;
* передаваемые данные;
* адрес местоназначения (destination), идентифицирующий компьютер-получатель;
* инструкции сетевым компонентам о дальнейшем маршруте данных;
* информация компьютеру-получателю о том, как объединить передаваемый пакет с остальными, чтобы получить данные в исходном виде;
* информация для проверки ошибок, обеспечивающая корректность передачи.

Компоненты пакета группируются в три раздела: заголовок, данные и трейлер.



**Компоненты пакета**

**Заголовок**

Заголовок включает:

* сигнал, «сообщающий» о том, что передается пакет;
* адрес источника;
* адрес местоназначения;
* информацию, синхронизирующую передачу.

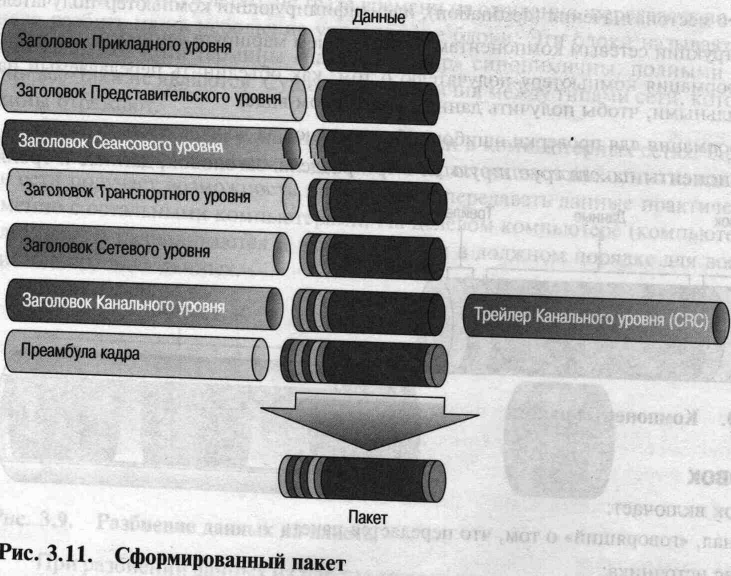
**Данные**

Эта часть пакета **–** собственно передаваемые данные. В зависимости от типа сети ее размер может меняться. Но для большинства сетей он составляет от 512 байтов (0,5 Кб) до 4 Кб.

Так как обычно размер исходных данных гораздо больше 4 Кб, для помещения в пакет их необхо­димо разбивать на меньшие блоки. При передаче объемного файла может потребоваться много паке­тов.

**Трейлер**

Содержимое трейлера зависит от метода связи, или протокола. Впрочем, чаще всего трейлер содер­жит информацию для проверки ошибок, называемую циклическим избыточным кодом (Cyclical Re­dundancy Check, CRC). CRC **–** это число, получаемое в результате математических преобразований над пакетом и исходной информацией. Когда пакет дос­тигает местоназначения, эти преобразования повторяются. Если результат совпадает с CRC, то пакет принят без ошибок. В противном случае при передаче данные изменились, поэтому необходимо повторить передачу пакета.



Формат и размер пакета зависят от типа сети. А максимальный размер пакета определяет, в свою очередь, количество пакетов, которое будет создано сетевой операционной системой для передачи большого блока данных.

**Формирование пакетов**

***Процесс формирования пакета начинается на Прикладном уровне модели OSI, там, где «рожда­ются» данные.*** Информация, которую надо передать по сети, проход сверху вниз все семь уровней, начиная с Прикладного. На каждом уровне компьютера-отправителя к блоку данных добавляется информация, предназначенная для соответствующего уровня компьютера‑получателя. Например, информа­ция, добавленная на Канальном уровне компьютера-отправителя, будет прочитана Канальным уров­нем компьютера-получателя. Транспортный уровень разбивает исходный блок данных на пакеты. Структура пакетов определяется протоколом, который используют два компьютера – получатель и отправитель.

На Транспортном уровне, кроме того, к пакету добавляется информация, которая поможет компью­теру-получателю восстановить исходные данные из последовательно­сти пакетов.

Когда, завершив свой путь к кабелю, пакет проходит Физический уровень, он содержит информацию всех остальных шести уровней.

**Адресация пакета**

Большинство пакетов в сети адресуется конкретному компьютеру, и, как результат, только он один реагирует на них. Каждая плата сетевого адаптера «видит» все пакеты, передаваемые по сегменту кабеля, но только при совпадении адреса пакета с адресом компьютера она прерывает его работу. Используется также и широковещательная адресация (broadcast addressing). На пакет с таким типом адреса одновременно реагируют множество компьютеров в сети.

В крупномасштабных сетях, покрывающих огромные территории (или государства), предлагается несколько возможных маршрутов для передачи данных. Коммутирующие и соединяющие сетевые компоненты используют адресную информацию пакетов для определения наилучшего из маршру­тов.

**Рассылка пакетов**

Сетевые компоненты используют адресную информацию пакетов и для других целей: чтобы направлять пакеты по назначению и не допускать их вте области сети, к которым они не относятся. В правильной рассылке пакетов ключевую роль играют две функции:

* *Продвижение пакетов.* Компьютер может отправить пакет на следующий подходящий сетевой компонент, основываясь на адресе из заголовка пакета;
* *Фильтрация пакетов.* Компьютер может отбирать определенные пакеты на основе некоторых критериев, например, адреса.

Самый нижний (уровень IV) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений "точка-точка" SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP за счет разработки соответствующего RFC, определяющего метод инкапсуляции пакетов IP в ее кадры.

Следующий уровень (уровень III) - это уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий локальных сетей, территориальных сетей, линий специальной связи и т. п.

В качестве основного протокола сетевого уровня (в терминах модели OSI) в стеке используется протокол IP, который изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

**К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.**

Следующий уровень (уровень II) называется основным. На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

Верхний уровень (уровень I) называется прикладным. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся такие широко используемые протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие. Остановимся несколько подробнее на некоторых из них.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за счет использования для такого доступа предопределенного имени пользователя Anonymous.

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол - простейший протокол пересылки файлов TFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения - UDP.

Протокол telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Поэтому серверы telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например, систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Изначально протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet, которые традиционно часто называют также шлюзами. С ростом популярности протокол SNMP стали применять и для управления любым коммуникационным оборудованием - концентраторами, мостами, сетевыми адаптерами и т.д. и т.п. Проблема управления в протоколе SNMP разделяется на две задачи.

Первая задача связана с передачей информации. Протоколы передачи управляющей информации определяют процедуру взаимодействия SNMP-агента, работающего в управляемом оборудовании, и SNMP-монитора, работающего на компьютере администратора, который часто называют также консолью управления. Протоколы передачи определяют форматы сообщений, которыми обмениваются агенты и монитор.

Вторая задача связана с контролируемыми переменными, характеризующими состояние управляемого устройства. Стандарты регламентируют, какие данные должны сохраняться и накапливаться в устройствах, имена этих данных и синтаксис этих имен. В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.