

ЛЕКЦИЯ 6:

«Стеки коммуникационных протоколов»

1. Понятие стека коммуникационных протоколов.
2. Стеки популярных коммуникационных протоколов.
3. Спецификации стандартов в области компьютерных сетей.

1. Понятие стека коммуникационных протоколов.

Коммуникационный протокол является одним из важнейших элементов архитектуры сети и представляет собой формализованный **набор правил взаимодействия узлов сети**.

Протокольные **сущности** двух взаимодействующих узлов сети –это **программные модули**, реализующие процедуры взаимодействия, которые обмениваются сообщениями в соответствии с определенным для них коммуникационным **протоколом**.

Сообщения в виде порций потоков данных состоят из полей **служебной информации** (заголовков и концевиков) и полей собственно передаваемой информации – полей **данных**. Сообщения, которые обеспечивают **выполнение правил** информационного **взаимодействия** узлов сети могут и **не содержать** полей данных.

Иерархически организованный **набор протоколов**, который **достаточен** для **обеспечения взаимодействия** узлов в сети с целью решения поставленной задачи или совокупности поставленных задач называется **стеком протоколов**.

В зависимости от технологий построения сетей различают большое количество стеков коммуникационных протоколов, которые являются **открытыми**, т.е. **общедоступными**, **согласованными** с производителями и пользователями, или **стандартизованными** и **представленными в форме открытых спецификаций**.

Под **спецификацией протокола** понимается детальное перечисление и формальное описание процедур взаимодействия **протокольных сущностей**.

В настоящее время **наиболее известными** являются протоколы и стеки протоколов, такие как:

- **OSI** (Open System Interconnection – стек протоколов взаимодействия открытых систем);

- **TCP/IP** (Transmission Control Protocol /Internet Protocol – протокол управления передачей/ межсетевой (интернет) протокол);

- **IPX/SPX** (Internetwork Packet Exchange/Sequenced Packet Exchange – стек протоколов межсетевого пакетного обмена /упорядоченного (транспортного) пакетного обмена), который представляет собой стандарт фирмы Novell для сетевой операционной системы OS Net Ware и долгое время занимал лидирующее положение при создании локальных компьютерных сетей);

- **NetBIOS** (Network Basic Input/Output System – стек протоколов сетевого расширения стандартных функций базовой системы ввода/вывода BIOS для сетевой программы PC Network фирмы IBM);

- **SNAP** (SubNetwork Access Protocol - протокол доступа к подсетям, который является вложенным в протокол канального уровня LLC) и др.

В большинстве из них на **нижних** уровнях модели OSI – **физическом и канальном**, используются **одни и те же** хорошо зарекомендовавшие себя **стандартизованные протоколы**, которые позволяют использовать в сетях **одну и ту же аппаратуру**. Например, на канальном уровне - X.25, Ethernet, OSI - 8802.x, на физическом - RS-232C, HDLC, LAP-B.

На **верхних** уровнях модели OSI различные стеки работают по своим **индивидуальным** протоколам, которые часто не соответствуют разбиению на уровни OSI.

В частности, функции **прикладного** уровня, а также уровней **представления и сеансового**, во многих стеках, бывают **объединены в один протокол**. Такими протоколами, например, являются:

- **SMB** - протокол прикладного уровня стека IBM Microsoft для реализации сетевой файловой службы;
 - **FTP и NFS** – протоколы сетевой файловой службы стека TCP/IP;
 - **NCP** - протокол сетевой файловой службы в ОС Novell Net Ware;
- и др.

Такое несоответствие связано с тем, что **эталонная модель OSI** появилась как **результат обобщения** уже **существующих** и широко **используемых на практике** стеков протоколов.

Важно различать **модель OSI** и **стек протоколов OSI**. Модель OSI – это концептуальная схема взаимодействия открытых систем, представляющая **декомпозицию** сложных задач взаимодействия аппаратно- программных средств, выстроенную по **иерархическому** принципу, а стек протоколов OSI – это набор спецификаций (**детального** описания всех **необходимых** функций) конкретных протоколов взаимодействия. В отличие от **других стеков** протоколов, стек протоколов OSI **полностью** соответствует модели OSI, включая спецификации протоколов для всех семи уровней. Разработчики стека OSI, в отличие от своих предшественников, напрямую **руководствовались моделью OSI**.

В таблице 1 представлено соответствие наиболее распространенных в настоящее время **стеков** протоколов уровням модели OSI.

Таблица 1

Уровень OSI и спецификации протоколов	Ключевые слова	Протокольные единицы данных - PDU	Основные функции и особенности процедур взаимодействия
Прикладной (FTP, X.400, SMTP, FTAM.)	Поток данных, разделение, массив.	Сообщение. (Массив данных)	Предоставляет вид сетевого сервиса: перенос файлов, обмен почтовыми сообщениями, доступ к веб-страницам, управление сетью и др.
Представления (FTP, X.400, SMTP, FTAM.)	Форма представления.	Сообщение. (Массив данных)	Устранение синтаксических различий в представлении данных. Шифрование, сжатие данных. Разметка сообщений.
Сеансовый (FTP, X.400, SMTP, FTAM.)	Диалог, сеанс, синхронизация работы.	Сегмент (TCP). Дейтаграмма (UDP).	Управление диалогом (обращений и ответов), синхронизация работы (по сеансам связи), поддержка вызовов удалённых процедур.
Транспортный (TCP, UDP, NCP, SPX.)	Надёжность, качество, контроль.	Сегмент (TCP). Дейтаграмма (UDP).	Надёжность передачи, гарантированная доставка, мультимплексирование данных «сверху вниз» и демультимплексирование «снизу вверх».
Сетевой (CLNP, IP, IPX, X.25.)	Коммутация, адресация, маршрутизация.	Пакет или дейтаграмма (IP).	Маршрутизация логических адресов, создание и введение таблиц маршрутизации, фрагментация и сборка данных. Межсетевое соединение.
Канальный (X.25, Ethernet, OSI- 8802.x)	Инкапсуляция, контроль ошибок, передача.	Кадр или фрейм.	Доставка по физическому адресу устройства, синхронизация кадров, доступ к среде передачи. Соединение внутри локальной сети.
Физический (RS-232C, HDLC, LAP-B)	Биты, модуляция, сигналы.	Биты	Синхронизация битов, модуляция сигналов, согласование электрических и механических характеристик узлов сети с линией передачи.

2. Стеки популярных коммуникационных протоколов.

2.1. Стек протоколов OSI

Следует различать эталонную **модель** OSI и **стек** протоколов OSI. Модель определяет **концептуально схему взаимодействия** открытых систем, а стек представляет **собой набор** вполне конкретных спецификаций протоколов. В отличие от других, широко применяемых на практике, стеков, **стек OSI** полностью соответствует модели ВОС и включает спецификации протоколов для всех семи уровней ее взаимодействия (Табл.1).

На **нижних** уровнях стек OSI **поддерживает** технологии локальных сетей: Ethernet, Token Ring, FDDI, для глобальных сетей протоколы X.25, ATM, СЦИ/SDH, ISDN и др. Протоколы **верхних** уровней - сетевого, транспортного и сеансового специфицированы и реализованы прикладными протоколами стека OSI, такими как, протоколы передачи файлов FTAM, эмуляции терминала VTP, справочной службы X.500, электронной почты X.400 и др.

Протоколы стека OSI отличаются **большой сложностью и неоднозначностью спецификаций** из-за их высокой **универсальности** и свойства **открытости** применительно ко всем существующим и вновь появляющимся сетевым технологиям.

Из-за сложности протоколы OSI требуют **больших затрат вычислительной мощности** центрального процессора и являются подходящими **для рабочих станций** крупных сетей, а **не для сетей** персональных компьютеров.

Стек протоколов OSI – это **международный стандарт**, не зависящий от различных производителей сетевого оборудования. Поддерживается правительством США и там почти **не осталось** старых сетей, работающих по собственным протоколам. Стек OSI **популярен** в Европе и России, и имеет статус международного.

В отличие от других протоколов стек OSI **полностью соответствует 7-и уровневой модели** взаимодействия открытых систем и включает спецификации для всех уровней этой модели (Рис.1).

На физическом и канальном уровнях стек OSI поддерживает – т.е. способен реализовать функции всех, разработанных ранее, популярных протоколов нижних уровней (Ethernet, X.25, FDDI и др.).

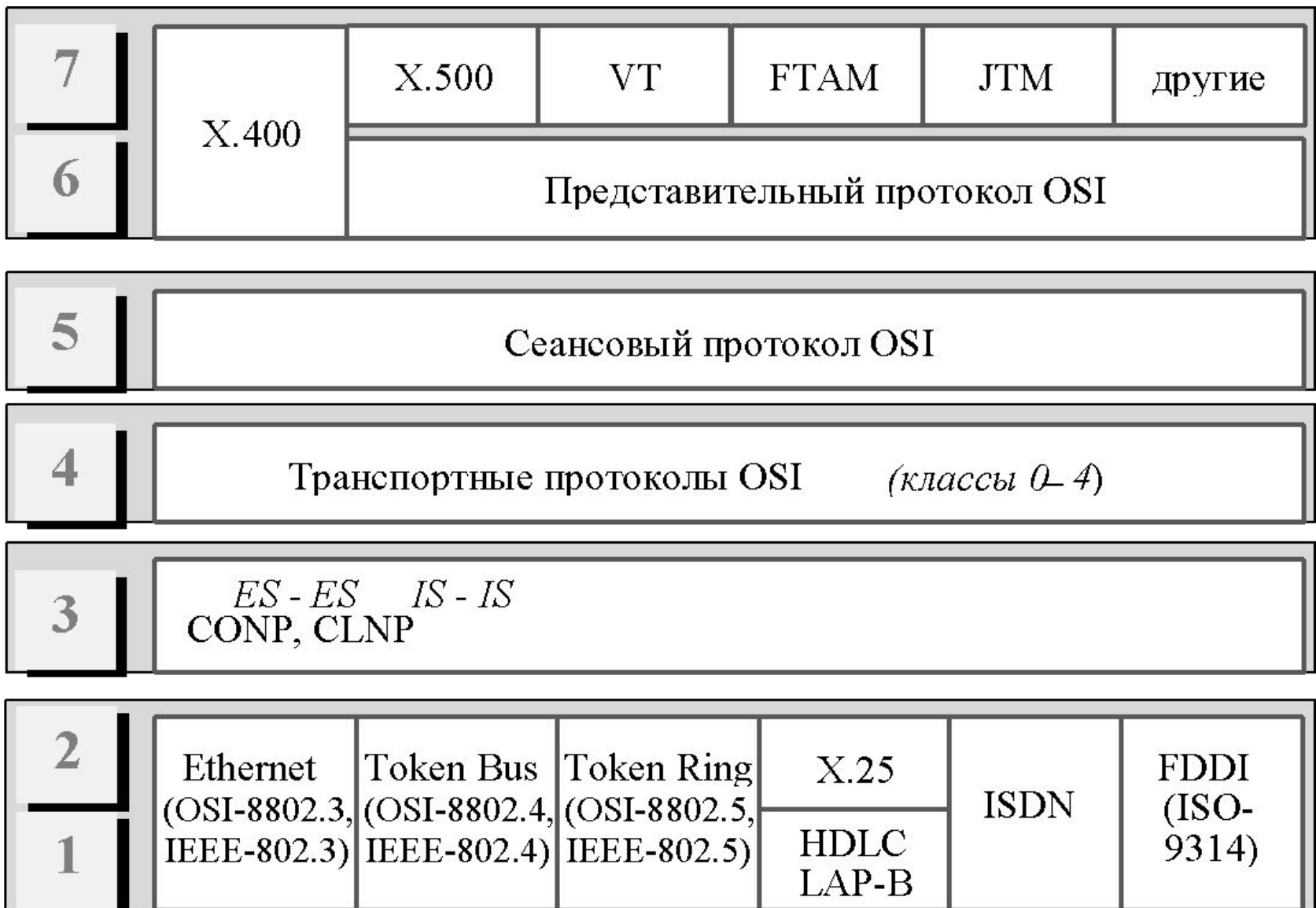
На сетевом уровне стек OSI использует протоколы CONP и CLNP – ориентированные и не ориентированные на соединение.

Транспортные протоколы уникальны и предполагают задание требуемого уровня обслуживания от 0 до 4.

Сеансовый уровень представлен только своим уникальным протоколом OSI.

Уровень представления помимо уникального содержит протокол электронной почты X.400.

На прикладном уровне в стек включены (поддерживаются) службы: каталогов (X.500); электронная почта (X.400); протокол виртуального терминала (VTP); протокол передачи, доступа и управления файлами (FTAM); протокол управления работой сети (JTM).



Уровни
модели
OSI

1. Стек протоколов OSI, включающий разработанные вне стека наиболее популярные протоколы нижних и верхнего уровней.

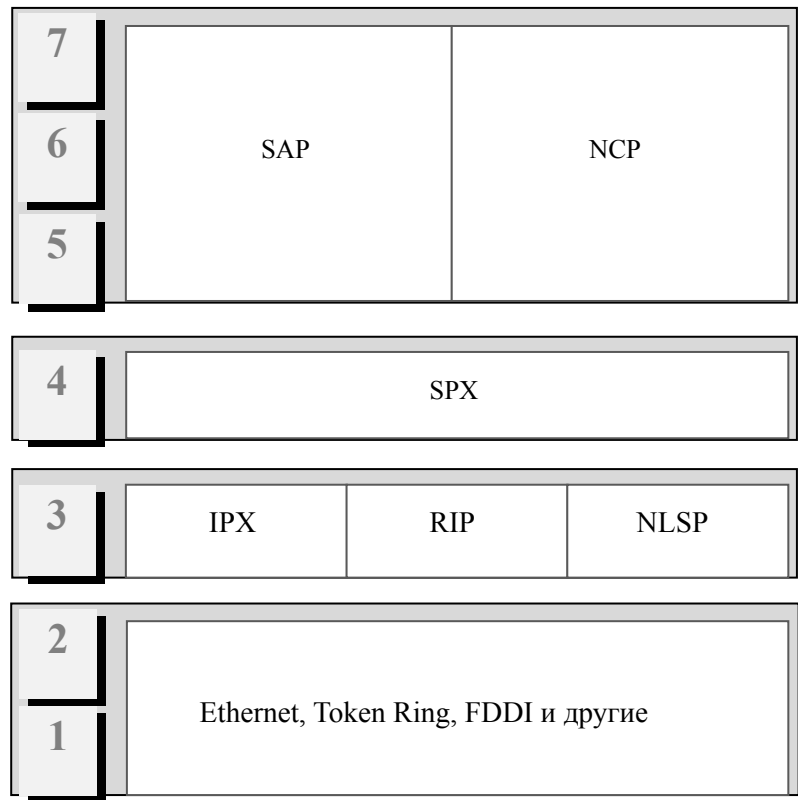
2.2. Стек протоколов IPX/SPX .

Этот стек **компании Novell** разработан для сетевой операционной системы NetWare еще в начале 80-х годов. Название стеку дали протоколы сетевого и сеансового уровней IPX (Internetwork Packet Exchange) и SPX (Sequenced Packet Exchange). Популярность стека IPX/SPX связана с **популярностью** операционной системы **ОС Net Ware**, которая до недавнего времени сохраняла мировое лидерство в локальных сетях, состоящих из **ПК со скромными системными ресурсами** (процессор, память, общая шина и др.).

Многие особенности стека IPX/SPX обусловлены ориентацией ОС Net Ware ранних версий на **работу** в локальных **сетях небольших размеров**, из-за чего протоколы стека IPX/SPX хорошо работали в локальных и не очень хорошо в больших корпоративных сетях, так как слишком **перегружали** медленные глобальные межсетевые связи **широковещательными пакетами**, которые интенсивно используются несколькими протоколами этого стека. Это ограничивает его применение локальными сетями, не разделенными на подсети, и делает невозможным использование его в составных сетях. Некоторые ограничения NetBEUI снимаются реализацией этого протокола NBF (NetBEUI Frame), которая включена в ОС Microsoft Windows NT. На рисунке (Рис.2 б) приведена структура стека NetBIOS/SMB в соответствии с моделью OSI.

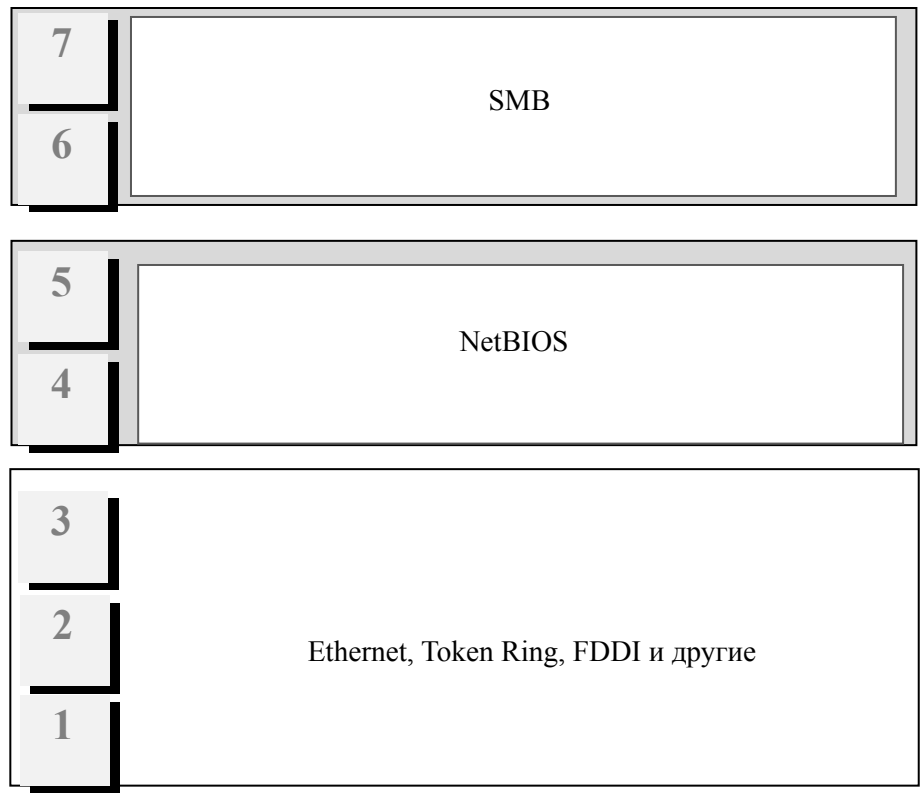
Однако с момента выпуска ОС версии **Net Ware 4.0** компания Novell внесла и продолжает вносить в свои протоколы серьезные изменения, направленные на их адаптацию для работы в **больших** корпоративных сетях.

В настоящее время стек протоколов IPX/ SPX (Рис.2 а) **реализован** не только в ОС Net Ware, но и **в других** популярных сетевых ОС, например, UNIX, Microsoft Windows NT.



Уровни модели OSI

а).



Уровни модели OSI

б).

Рис. 2. Структура стеков протоколов; а). IPX/SPX ; б). NetBIOS/SMB.

2.3. Стек протоколов NetBIOS/SMB

Стек протоколов NetBIOS/SMB широко используется в продуктах **компаний IBM и Microsoft**. На физическом и канальном уровнях в качестве протоколов этого стека используются наиболее распространенные протоколы Ethernet, Token Ring, FDDI. На верхних уровнях работают протоколы NetBEUI и SMB (Server Message Block).

Протокол NetBIOS (Network Basic Input/Output System) этого стека появился в 1984 г. **как расширение стандартных функций базовой системы** ввода/вывода (BIOS) IBM PC для сетевой программы PC Network компании IBM. В дальнейшем этот протокол был заменен **протоколом расширенного пользовательского интерфейса** NetBEUI (NetBIOS Extended User Interface). Для обеспечения совместимости приложений в качестве интерфейса к протоколу NetBEUI был сохранен интерфейс NetBIOS.

Протокол NetBEUI разрабатывался как эффективный, потребляющий немного ресурсов и предназначенный для сетей, насчитывающих не более 200 рабочих станций. Этот протокол содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI, однако с его помощью **невозможна маршрутизация пакетов**.

2.4. Стек протоколов TCP/IP.

Стек протоколов TCP/IP был разработан по инициативе Министерства обороны США для связи экспериментальной сети ARPAnet с другими сетями как набор **общих протоколов для разнородной вычислительной среды**. Этот стек используется для связи компьютеров глобальной сети Internet, а также в огромном числе **корпоративных** сетей.

На нижнем уровне **стек поддерживает все распространенные стандарты физического и канального уровней**. Для локальных сетей - это Ethernet, Token Ring, FDDI, а для глобальных – протоколы работы на аналоговых и цифровых коммутируемых и выделенных линиях SLIP, PPP; протоколы глобальных сетей X.25 и ISDN, ATM и SONEN / SDH.

Основными протоколами стека, давшими ему название, являются протоколы **IP** (Internet Protocol – протокол составных сетей) и **TCP** (Transmission Control Protocol – протокол управления передачей), которые в терминологии модели OSI относятся к сетевому и транспортному уровням. Протокол IP **передает пакеты** по составной сети, а протокол TCP гарантирует **надежность** их доставки.

Наряду с протоколом TCP на транспортном уровне используется **UDP** (User Datagram Protocol) – **протокол передачи пользовательских дейтаграмм** (пакетов), не ориентированный на установление соединения.

Для обеспечения доставки дейтаграмм он использует адрес порта, являющегося указателем процесса, а не идентификатором соединения, как в TCP. Меньшие непроизводительные потери делают этот протокол более эффективным, чем TCP для дейтаграммной передачи.

Стек протоколов TCP/IP **вобрал в себя** большое число протоколов **прикладного уровня**. К ним относятся такие популярные протоколы, как протокол пересылки файлов FTP (File Transfer Protocol - протокол обмена файлами), протокол эмуляции терминала Telnet, почтовый протокол SMTP (Simple Mail Transfer Protocol – протокол обмена почтовыми сообщениями), используемый в электронной почте сети Интернет, гипертекстовые сервисы службы WWW (всемирной паутины) и др.

В настоящее время стек протоколов TCP/IP – **один из самых распространенных стеков транспортных протоколов** в локальных, глобальных и магистральных телекоммуникационных сетях.

Стремительный рост популярности Internet привел к тому, что протоколы **TCP/IP** в значительной мере **вытесняют** стек протоколов **IPX/SPX** компании Novell, необходимый, в первую очередь, для доступа к **файловым серверам NetWare**.

Процесс становления стека протоколов TCP/IP в качестве стека номер один в любых сетях **продолжается**, и в настоящее время разрабатываемые промышленные операционные системы **обязательно включают** программную реализацию этого стека.

Наряду с этим существует **большое количество локальных, корпоративных и территориальных сетей**, непосредственно **не входящих** в Internet, но в которых также используют протоколы TCP/IP. Чтобы отличать их от сети Internet, эти сети называют сетями TCP/IP, или просто **IP-сетями**.

Приложения пользователей для работы в Internet используют протоколы стека TCP/IP **верхнего уровня**, например передачу файлов или электронную почту.

Протокол **FTP** (Faile Transfer Protocol – протокол обмена файлами) применяется для передачи файлов между узлами сети Internet. Кроме этого, он позволяет пользователям взаимодействовать с удаленной системой. Этот протокол работает на трех верхних уровнях модели OSI.

На сеансовом уровне он администрирует сеанс, устанавливает соединение, передает файлы и закрывает соединение.

На уровне представления выполняет трансляцию файлов.

На прикладном уровне предлагает сетевые службы, а именно файловые и средства коллективной работы.

Протокол FTP **одноранговый**, позволяет передавать файлы между разнородными узлами, поскольку использует **общую файловую структуру, не зависимую от операционных систем**.

Протокол **Telnet** (протокол эмуляции терминала) используют **для эмуляции** (создания искусственных «заменителей» на функциональном уровне) **удаленных терминалов**.

Служба **Telnet** позволяет пользователям обращаться к приложениям удаленной системы путем эмуляции одного из ее терминалов.

Кроме того, протокол Telnet поддерживает соединение между различными операционными системами, работая на верхних трех уровнях модели OSI, а на сеансовом уровне обеспечивает управление диалогом, используя полудуплексный метод. На уровне представления он выполняет трансляцию сообщений, используя последовательность байтов и коды символов. На прикладном уровне предлагает функции поддержки удаленных операций.

Протокол **SMTP** (Simple Mail Transfer Protocol) – упрощенный протокол передачи электронной почты, маршрутизирующий почтовые сообщения. Он работает на прикладном уровне и обеспечивает средства обмена сообщениями. Протокол SMTP не предусматривает пользовательского интерфейса для приема и передачи сообщений, однако его поддерживают многие приложения электронной почты Internet. Для передачи почтовых сообщений в сети Internet протокол SMTP использует протоколы TCP и IP.

Поскольку стек TCP/IP изначально создавался для глобальной сети Internet, он имеет ряд преимуществ перед другими стеками, когда речь заходит о построении сетей, включающих глобальные связи. В частности, очень полезной является его способность фрагментировать пакеты.

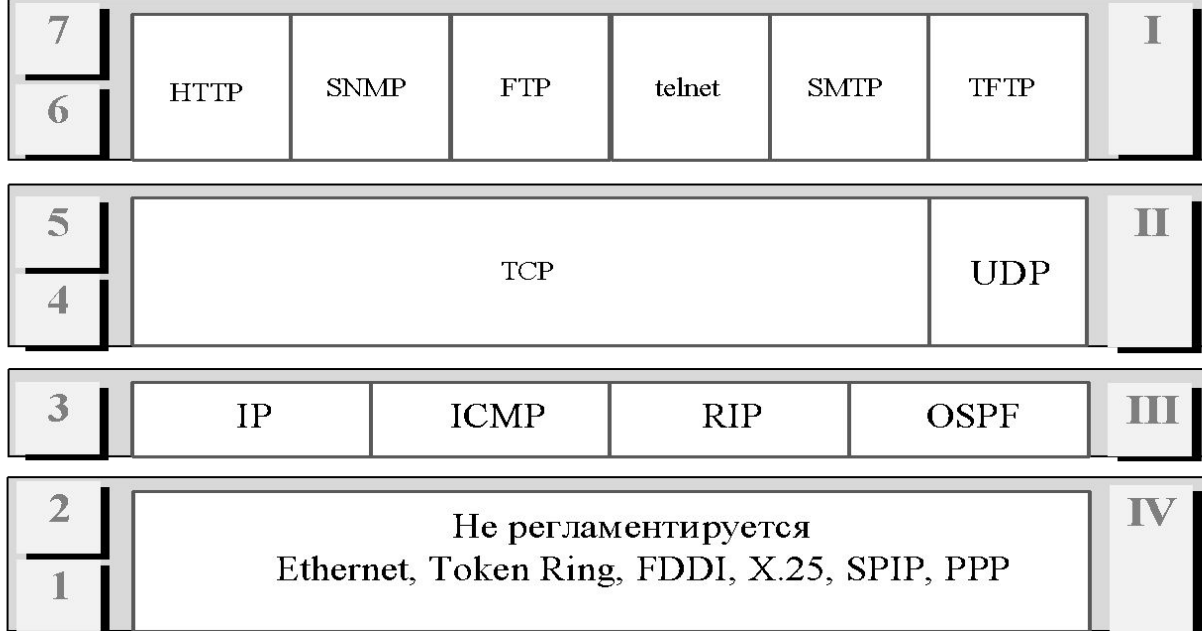
Эта возможность оказывается весьма важной для его применения в интернет-сетях, построенных по совершенно разным принципам. В каждой из сетей входящих в интернет-сеть, можно задать собственное значение максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из сети, имеющей большую максимальную длину кадра, в сеть с меньшей максимальной длиной кадра, возникает необходимость деления передаваемого кадра на несколько частей, что весьма эффективно обеспечивает протокол IP стека TCP/IP, который использует протокол SMTP.

Другой особенностью технологии TCP/IP является гибкая система адресации.

Преимущества, которые дает стек протоколов TCP/IP для построения сетей, неразрывно связаны с высокими требованиями, предъявляемыми к ресурсам, и сложностью администрирования IP-сетей. Мощные функциональные возможности протоколов стека TCP/IP требуют для своей реализации больших вычислительных ресурсов и затрат.

Реализация гибкой системы адресации и отказ от широковещательных рассылок приводят к наличию в IP-сети различных централизованных служб типа DNS, DHCP и т.п.

Каждая из этих служб предназначена для облегчения администрирования сети, включая конфигурирование сетевого оборудования. Архитектура стека TCP/IP представлена на рисунке (Рис. 3а), а названия PDU – на рисунке (Рис. 3б).



Уровни модели OSI

Уровни стека TCP/IP

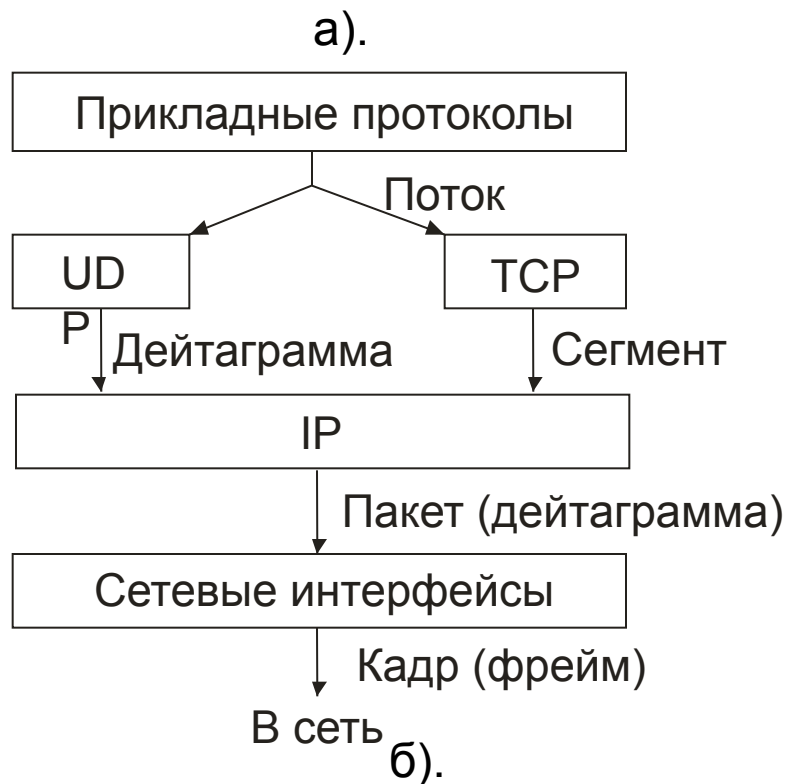


Рис. 3. Стек TCP/IP.

На рисунке (Рис. 4) приведен состав рассмотренных стеков протоколов и их соответствие уровням модели OSI. Можно заметить, что это соответствие весьма условно и вызвано тем, что разработчики стеков отдавали предпочтение скорости выполнения процедур взаимодействия в ущерб модульности построения. Кроме стека OSI ни один стек не разбит на 7 уровней.

Чаще всего в широко применяемых на практике стеках явно выделяются **3-4 обобщенных уровня**:

- **первый** - включает протоколы физического и канального уровней, которые аппаратно поддерживаются сетевыми адаптерами;
- **второй** – является сетевым;
- **третий** – включает протоколы транспортного;
- **четвертый** – соответствует уровню служб, включающий функции сеансового уровня, уровня представлений и прикладного.

В соответствии с **идеальной** моделью OSI в стеках протоколов **при переходе от более высокого к более низкому уровню PDU вышележащего уровня должна инкапсулироваться в PDU нижележащего**. Это обстоятельство на практике приводит к необходимости пересматривать уже существующие и хорошо зарекомендовавшие себя протоколы, разработанные в период до принятия концепции OSI.

Модель OSI	IBM/ Microsoft	TCP/IP	Novell	Стек OSI
Прикладной	SMB	Telnet, FTP, SNMP, SMTP, WWW	NCP, SAP	X.400 X.500 FTAM
Представления				Представ. протокол OSI
Сеансовый	NetBIOS	TCP	SPX	Сеансов. протокол OSI
Транспортный				Трансп. протокол OSI
Сетевой	IP, RIP, OSPF		IPX, RIP, NLSP	ES-ES IS-IS
Канальный	802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP			
Физический	Коаксиал, экранированная и неэкранированная витая пара, оптоволокно, радиоволны			

Рис.6.4. Соответствие популярных стеков протоколов модели OSI.

2.5. Современные сетевые протоколы

2.5.1 Протокол GPRS

Протокол GPRS. Изложение классических основ сетевых протоколов и их стандартов завершим рассмотрением некоторых современных сетевых протоколов различных уровней, имеющих особенно важное практическое значение. В данном разделе рассмотрим протокол GPRS.

GPRS (General Packet Radio Service) - протокол беспроводной радиосвязи уровня связывания данных (уровня 2) по модели ISO, широко используемый в мобильной связи (GSM). Данный протокол "понимает" структуру IP-пакетов. Обеспечивается реальная скорость связи до 60 КБит / с, сравнимая со скоростью обычного модема и обмена через телефонную линию (dial-up).

Используется для реализации **SMS (текстовых сообщений)**, **MMS (мультимедийных сообщений)**, **Instant messaging and presence (отправки и получения мгновенных сообщений)**, **WAP (упрощенного доступа к Web для мобильных телефонов)**, мобильного Интернета

В некоторых местностях и странах GPRS является фактически единственным способом организации связи для передачи данных и выхода в Интернет. Настоятельно рекомендуется при выборе мобильного телефона обращать внимание на поддержку протокола GPRS.

При использовании TCP/IP GPRS-протокол присваивает каждому мобильному телефону один или несколько IP-адресов и обеспечивает надежную пересылку IP-пакетов. IP-адреса, как правило, присваиваются динамически.

Для маршрутизации пакетов используются точки доступа (access points) со своими именами Access Point Names (APNs). При настройке GPRS в мобильном телефоне необходимо указать APN, предоставляемое Вашим провайдером (например, МТС)

При использовании телефона как GPRS-модема (для выхода в Интернет, приема электронной почты и т.д.) связь с компьютером осуществляется через Bluetooth или через инфракрасный порт (IrDA).

Не следует путать GPRS с GPS (глобальной системой спутниковой навигации), как иногда делают, в чем неоднократно убеждался автор.

Схема функционирования протокола GPS изображена на рис.5.

При использовании TCP/IP GPRS-протокол присваивает каждому мобильному телефону один или несколько IP-адресов и обеспечивает надежную пересылку IP-пакетов. IP-адреса, как правило, присваиваются динамически.

Для маршрутизации пакетов используются точки доступа (access points) со своими именами Access Point Names (APNs). При настройке GPRS в мобильном телефоне необходимо указать APN, предоставляемое Вашим провайдером (например, МТС)

При использовании телефона как GPRS-модема (для выхода в Интернет, приема электронной почты и т.д.) связь с компьютером осуществляется через Bluetooth или через инфракрасный порт (IrDA).

Не следует путать GPRS с GPS (глобальной системой спутниковой навигации), как иногда делают, в чем неоднократно убеждался автор.

Схема функционирования протокола GPS изображена на рис.5.

Устройства GPRS



Рис. 5. Протокол GPRS: Схема работы.

Семейство протоколов Wi-Fi (IEEE 802.11x)

Wi-Fi (IEEE 802.11x) – это семейство протоколов уровня связывания данных (уровня 2 по модели ISO) для беспроводной радиосвязи в локальных сетях (WLAN). Другое неофициальное (более старое) название того же семейства протоколов – **RadioEthernet**.

Используется для выхода в Интернет, **передачи голосовых сообщений через TCP/IP (VoIP)**, связи с мультимедийными устройствами (цифровыми камерами, проекторами и т.п.)

Скорость передачи данных – от 11 МБит / с (по стандарту 802.11b) до 54 МБит/с (по стандартам 802.11a и 802.11c).

Wi-Fi - связь доступна в радиусе действия **точки доступа (access point)** ~ 200-250 метров. Зона доступа Wi-Fi носит название **hotspot**. Типичная зона доступа – гостиница, аэропорт, вокзал, Интернет-кафе. Wi-Fi – адаптеры встраиваются в портативные компьютеры, органайзеры (PDA), коммуникаторы.

Преимущества Wi-Fi: при наличии точки доступа в соответствующей окрестности, доступ в Интернет возможен везде.

Недостатки Wi-Fi: локальный характер связи; различие числа Wi-Fi каналов в Европе, Америке и Азии; недостаточная безопасность; на практике, недостаточная надежность при числе пользователей 1000 – 10000 и более; связь Wi-Fi не безвредна для здоровья (поэтому ограничена для использования в странах Евросоюза).

Wi-MAX – более высокоскоростной вариант Wi-Fi (со скоростью передачи данных до 1 Гбит / с) с большим радиусом действия. В настоящее время отечественные коммуникационные фирмы активно ведут работу по покрытию территории РФ сетями Wi-MAX.

Обмен мгновенными сообщениями (Instant Messaging and Presence)

Instant Messaging and Presence (IMP) - семейство протоколов и технологий

верхнего уровня (application layer) для обмена сообщениями между клиентами, использующими мобильные телефоны, коммуникаторы, ноутбуки и перемещающимися из одной точки в другую.

IMP использует адреса, сходные с email-адресами, например: **node@domain/work** – XMPP-адрес.

Посылаемые сообщения – как правило, текстовые, но также возможно посылать и графические образы.

Основные понятия IMP: **IMP client** – пользователь сети; **presence** – информация о присутствии клиента на связи; **presentity (presence server)** – сервер сети, обеспечивающий регистрацию клиентов и выдачу информации о присутствии на связи.

Основные протоколы IMP: **SIMPLE / SIP; XMPP (Jabber); Wireless Village.**

Лаборатория Java-технологии СПбГУ под научным руководством автора в 2003 – 2006 гг. выполнила работы для лаборатории Panasonic Research по реализации Java-библиотек для мгновенных сообщений (JSR 164 / 165 / 186 / 187) и разработке комплексов тестов для их тестирования (TCKs).

Основные функции протоколов канального уровня (пример).

Канальный уровень локальных сетей разбит на два подуровня:

- подуровень связи логических каналов (LLC – Logical Link Connection) или его ещё называют – уровень соединения канала передачи данных (DLC – Data Link Connection).
- подуровень управления доступом к среде передачи (MAC – Media Access Control).

Протоколы подуровней MAC и LLC взаимно не зависимы.

MAC-подуровень обеспечивает совместное использование общей среды, предоставляя её в распоряжение той или иной станции сети в соответствии с определенным алгоритмом. После того как получен доступ к среде, ею может пользоваться следующий подуровень, организующий надежную передачу кадров.

LLC-подуровень отвечает за достоверную передачу кадров данных между узлами, а также реализует функции интерфейса с прилегающим сетевым уровнем.

Протоколы подуровня LLC обеспечивают нужное качество услуг (сервис) для протоколов вышестоящего уровня. Протокол сетевого уровня передает для протокола LLC следующую информацию:

пакет данных (IP, IPX и т.д.);

адресную информацию об узле назначения;

требования к качеству услуг.

Протокол LLC – протокол управления логическим каналом. Обеспечивает сервис трех типов:

LLC1 – сервис без установления соединения и без подтверждения;

LLC2 – с установлением соединения и подтверждением;

LLC3 – без установления соединения, но с подтверждением.

Процедура LLC1 определяет обмен данными без предварительного установления соединения и без повторной передачи кадров в случае обнаружения ошибочной ситуации, то есть является процедурой дейтаграммного типа. Именно этот тип процедуры и используется во всех практических реализациях Ethernet. Поле управления для этого типа процедур имеет значение 03, что определяет все кадры как нумерованные. Дает пользователю средство для передачи данных с минимальными издержками. Используется, когда функции восстановления данных после ошибок и их упорядочивание выполняется протоколами высших уровней.

Процедура LLC2 определяет режим обмена с установлением соединений, нумерацией кадров, управлением потоком кадров и повторной передачей ошибочных кадров. Работает в режиме скользящего окна. В локальных сетях Ethernet этот режим используется редко. Повышает надежность передачи данных, но часто приводит к неоправданной избыточности.

Процедура LLC3 определяет режим передачи данных без установления соединения, но с получением подтверждения о доставке информационного кадра адресату. Только после этого может быть отправлен следующий информационный кадр. Используется в сетях с системой управления промышленными объектами в реальном времени, когда временные издержки установления логического соединения неприемлемы, а подтверждение корректности приема данных необходимо.

Чаще всего в ЛС используется сервис LLC1, так как кабельные каналы обеспечивают низкую вероятность ошибки и потери кадров. В конкретных устройствах могут поддерживаться несколько типов сервиса:

устройства класса I поддерживают только LLC1;

устройства класса II поддерживают LLC1 и LLC2;

устройства класса III поддерживают LLC1 и LLC3;

устройства класса IV поддерживают LLC1, LLC2 и LLC3;

Кадры подуровня LLC – блоки данных – Protocol Data Unit – PDU – делятся на три типа:

– информационные кадры, предназначенные для передачи информации в процедурах с установлением логического соединения; содержат информационное поле; в процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна;

– управляющие кадры, предназначенные для передачи команд и ответов в процедурах с установлением логического соединения, в том числе и запросов на повторную передачу искаженных информационных блоков;

– нумерованные кадры, предназначенные для передачи нумерованных команд и ответов в процедуре без установления логического соединения, передачи информации, идентификации и тестирования LLC-подуровня; в процедурах с установлением логического соединения используются для установления и разъединения логического соединения и передачи информации об ошибках.

Все типы кадров подуровня LLC имеют единый унифицированный формат, показанный на рисунке 6.5.

1 байт	1 байт	1 байт	1 байт		1 байт
флаг 01111110	DSAP	SSAP	Control	Data	флаг 01111110

Рисунок 6.5 – Формат кадра LLC

DSAP – Destination Service Access Point – адрес точки доступа сервиса назначения;

SSAP – Source Service Access Point – адрес точки доступа сервиса источника;

Control – поле управления, задает тип кадра LLC-подуровня, а так же порядковый номер кадра в режиме с установлением соединения;

Data – поле данных для размещения данных протоколов верхнего уровня, в некоторых управляющих и нумерованных кадрах может отсутствовать;

Флаг – однобайтовое поле, используемое на MAC-подуровне для определения границ блоков данных.

Поля DSAP, SSAP указывают, какой сервис верхнего уровня посылает данные с помощью этого кадра, то есть на приеме необходимо распознавать, какой протокол вложил свой пакет в поле данных, чтобы передать извлеченный из кадра пакет нужному протоколу для дальнейшей обработки.

Протоколы прикладного уровня.

Прикладные протоколы работают на верхнем уровне модели OSI. Они обеспечивают взаимодействие приложений и обмен данными между ними. К наиболее популярным прикладным протоколам относятся:

- APPC (Advanced Program-to-Program Communication) - одноранговый SNA-протокол фирмы IBM, используемый в основном на AS/400;
- FTAM (File Transfer Access and Management) - протокол OSI доступа к файлам;
- X.400 - протокол CCITT для международного обмена электронной почтой;
- X.500 - протокол CCITT служб файлов и каталогов на нескольких системах;
- SMTP (Simple Mail Transfer Protocol) - протокол Интернета для обмена электронной почтой;
- FTP (File Transfer Protocol) - протокол Интернета для передачи файлов;
- SNMP (Simple Network Management Protocol) - протокол Интернета для мониторинга сети и сетевых компонентов;
- Telnet - протокол Интернета для регистрации на удаленных хостах и обработки данных на них;

- Microsoft SMBs (Server Message Blocks, блоки сообщений сервера) и клиентские оболочки или редиректоры;
- NCP (Novell NetWare Core Protocol) и клиентские оболочки или редиректоры фирмы Novell;
- Apple Talk и Apple Share - набор сетевых протоколов фирмы Apple;
- AFP (AppleTalk Filing Protocol) - протокол удаленного доступа к файлам фирмы Apple;
- DAP (Data Access Protocol) - протокол доступа к файлам сетей DECnet.

Протоколы транспортного уровня.

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данных между ними. К популярным транспортным протоколам относятся:

- TCP (Transmission Control Protocol) - TCP/IP-протокол для гарантированной доставки данных, разбитых на последовательность фрагментов;
- SPX - часть набора протоколов IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для данных, разбитых на последовательность фрагментов, фирмы Novell;
- NWLink - реализация протокола IPX/SPX от фирмы Microsoft;
- NetBEUI (NetBIOS - Network Basic Input/Output System);
- EUI (Extended User Interface) - расширенный интерфейс пользователя - устанавливает сеансы связи между компьютерами (NetBIOS) и предоставляет верхним уровням транспортные услуги (NetBEUI);
- ATP (AppleTalk Transaction Protocol), NBP (Name Binding Protocol) - протоколы сеансов связи и транспортировки данных фирмы Apple.

Протоколы сетевого уровня.

Сетевые протоколы обеспечивают услуги связи – **соединения на логическом уровне** узлов сети для передачи данных. Эти протоколы управляют несколькими типами данных: адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу. Сетевые протоколы, кроме того, определяют правила для осуществления связи в конкретных сетевых средах, например Ethernet или Token Ring. К наиболее популярным сетевым протоколам относятся:

- IP (Internet Protocol) - TCP/IP-протокол для передачи пакетов;

- IPX (Internetwork Packet Exchange) - протокол фирмы NetWare для передачи и маршрутизации пакетов;

- NWLink - реализация протокола IPX/SPX фирмой Microsoft;

- NetBEUI - транспортный протокол, обеспечивающий услуги транспортировки данных для сеансов и приложений NetBIOS;

- DDP (Datagram Delivery Protocol) - AppleTalk-протокол транспортировки данных.

Приложения

Телекоммуникационная сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных, в которой осуществляется последовательная бит-ориентированная передача информации (данных) между связанными друг с другом независимыми устройствами.

Различают два понятия сети: коммуникационная сеть и информационная сеть.

Коммуникационная сеть предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

Информационная сеть предназначена для хранения информации и состоит из информационных систем. На базе коммуникационной сети может быть построена группа информационных сетей.

Под **информационной системой** следует понимать систему, которая является поставщиком или потребителем информации.

Компьютерная сеть состоит из информационных систем и каналов связи.

Под информационной системой следует понимать объект, способный осуществлять хранение, обработку или передачу информации. В состав информационной системы входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных.

В дальнейшем информационная **система**, предназначенная для решения **задач пользователя**, будет называться – **рабочая станция** (client). Рабочая станция в сети отличается от обычного персонального компьютера (ПК) наличием **сетевой карты** (сетевого адаптера), **канала** для передачи данных и **сетевого программного** обеспечения.

Под **каналом** связи следует понимать путь или среду, по которому (- ой) передаются сигналы. Среда **передачи сигналов** называется абонентским, или физическим, каналом.

Каналы связи (data link) создаются по линиям связи при помощи сетевого **оборудования** и физических **сред** связи. Физические среды связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или радиосреды.

Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются **логические каналы**.

Логический канал – это **путь** для передачи данных от одной системы к другой. Логический канал прокладывается **по маршруту** в одном или нескольких **физических** каналах. **Логический канал** можно охарактеризовать, как **маршрут**, проложенный через физические каналы и узлы коммутации.

Информация в сети передается **блоками данных** по процедурам (формализованным правилам) обмена данными между объектами. Эти процедуры называют **протоколами** передачи данных.

Протокол – это совокупность формализованных правил, устанавливающих формат и алгоритм обмена информацией между двумя или несколькими устройствами.

Загрузка сети характеризуется параметром, называемым **трафиком**. Трафик (traffic) – это **поток сообщений** в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду.

Существенное влияние на характеристику сети оказывает метод доступа.

Метод доступа – это способ определения того, какая из рабочих станций сможет следующей использовать канал связи и как управлять доступом к каналу связи (кабелю).

В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой топологией. **Топология** – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Состав основных элементов в сети зависит от ее архитектуры.

Архитектура – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

В основном выделяют три вида архитектур: архитектура **терминал – главный компьютер**, архитектура **клиент – сервер** и **одноранговая** архитектура.

Современные сети можно классифицировать по различным признакам: по удаленности компьютеров, топологии, назначению, перечню предоставляемых услуг, принципам управления (централизованные и децентрализованные), методам коммутации, методам доступа, видам среды передачи, скоростям передачи данных и т. д.

Приложение : спецификации протокола IP.

Internet Protocol — межсетевой протокол. Относится к маршрутизируемым протоколам сетевого уровня семейства TCP/IP. Протокол IP используется **для негарантированной доставки данных** в виде пакетов от одного узла сети к другому. Это означает, что на уровне этого протокола (3-й уровень модели OSI) не даётся гарантий надёжной доставки пакета до адресата. В частности, пакеты могут прийти **не в том порядке**, в котором были отправлены, **продублироваться**, если приходят по разным маршрутам две копии одного пакета, что случается крайне редко, оказаться **повреждёнными** или **не прибыть** вовсе.

Гарантию безошибочной доставки пакетов дают протоколы более высокого (4-го - транспортного уровня) сетевой модели OSI, например, протокол TCP, который использует IP в качестве протокола для транспортировки пакетов.

В современной сети Интернет используется IP четвёртой версии - **IPv4**. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (4 байта).

При этом компьютеры в подсетях **объединяются общими начальными битами** адреса. Количество этих бит, **общее для данной подсети**, называется **маской подсети**. В более ранних версиях прототкола использовалось деление пространства адресов по классам — А, В, С; класс сети определялся диапазоном значений старшего октета и определял число адресуемых узлов в данной сети. В настоящее время используется бесклассовая адресация узлов в подсетях.

В настоящее время вводится в эксплуатацию **шестая версия** протокола - **IPv6**, которая **позволяет адресовать** значительно **большее количество узлов**, чем IPv4.

Эта версия отличается повышенной разрядностью адреса, встроенной **возможностью шифрования** и некоторыми другими особенностями. Переход с IPv4 на IPv6 связан с трудоёмкой работой операторов связи и производителей программного обеспечения и не может быть выполнен одномоментно. В 2010 года в Интернете присутствовало более 3000 сетей, работающих по протоколу IPv6. Для сравнения, на то же время в адресном пространстве IPv4 присутствовало более 320 тысяч сетей. Однако, в сетях, использующих протокол IPv6, гораздо больше абонентских узлов, нежели в сетях IPv4.

IP-пакет (дейтаграмма) – это **форматированный блок информации**, снабженный служебной информацией и передаваемый по телекоммуникационной или компьютерной сети.

Интернет-сети (составные), которые **не поддерживают передачу пакетов**, имеющие, например, традиционные соединения типа «точка-точка» в телекоммуникациях, просто **передают данные** в виде последовательности **байтов, символов или битов**.

При использовании пакетного форматирования (разбиения массива данных на части) **длинные сообщения** сеть может передавать **более надежно и эффективно**.

Основные протоколы TCP/IP по уровням модели OSI

Уровень 7 – Прикладной:

1. BGP • HTTP • HTTPS • DHCP • IRC • SNMP • DNS • DNSSEC • NNTP • XMPP • SIP • BitTorrent • IPP • NTP • SNTP;
2. Электронная почта SMTP • POP3 • IMAP4;
3. Передача файлов FTP • TFTP • SFTP;
4. Удалённый доступ rlogin • Telnet • RD.

Уровень 6 - Представления: XDR • SSL.

Уровень 5 - Сеансовый: ADSP • H.245 • iSNS • NetBIOS • PAP • RPC • L2TP • PPTP • RTCP • SMPP • SCP • SSH • ZIP • SDP.

Уровень 4 - Транспортный: TCP • UDP • SCTP • DCCP • RUDP • RTP.

Уровень 3 - Сетевой: IPv4 • IPv6 • IPsec • ICMP • IGMP • ARP • RARP • RIP2 • OSPF.

Уровень 2 - Канальный: Ethernet • PPPoE • PPP • L2F • 802.11 Wi-Fi • 802.16 WiMax • Token ring • ARCNET • FDDI • HDLC • SLIP • ATM • DTM • X.25 • Frame relay • SMDS • STP.

Уровень 1 - Физический: Ethernet • RS-232 • EIA-422 • RS-449 • RS-485.

Идеология протокола IP

Взаимодействие протоколов:

Протокол Internet (IP) взаимодействует с одной стороны с протоколами передачи информации между хост-компьютерами, а с другой - с протоколами локальной компьютерной сети. При этом локальная сеть может являться малой компьютерной сетью, участвующей в создании большой сети, такой как Internet.

Сценарий работы:

Схему действий для передачи датаграммы от одной прикладной программы к другой можно проиллюстрировать следующим образом. Предположим, что перенос будет включать прохождение одного промежуточного шлюза.

1. Отправляющая прикладная программа готовит свои данные и вызывает свой локальный Internet модуль для отправки этих данных в качестве датаграммы, а в качестве аргументов этого вызова передает адрес получателя и другие параметры.
2. Модуль Internet готовит заголовок датаграммы и стыкует с ним данные.
3. Модуль Internet определяет локальный сетевой адрес, соответствующий данному адресу Internet. В данном случае это адрес шлюза.
4. Модуль передает данную датаграмму и адрес в локальной сети в распоряжение интерфейса локальной сети.
5. Интерфейс локальной сети создает соответствующий этой сети заголовок и соединяет с ним датаграмму.

6. Затем он передает по локальной сети полученный таким образом результат.

7. Датаграмма достигает хост-компьютер, играющий роль шлюза и расположенный в вершине сети.

8. Интерфейс локальной сети отделяет этот заголовок и передает датаграмму на модуль Internet.

9. Модуль Internet определяет из Internet адреса, что датаграмма должна быть направлена на хост-компьютер во второй сети.

10. Модуль Internet определяет адрес хоста-получателя в локальной сети. Он обращается к интерфейсу локальной сети с тем, чтобы она переслала данную датаграмму по назначению.

11. Интерфейс создает заголовок локальной сети и соединяет с ним датаграмму, а затем результат направляет на хост-получатель.

12. На хосте-получателе интерфейс локальной сети удаляет заголовок локальной сети и передает оставшееся на Internet модуль.

13. Модуль Internet определяет, что рассматриваемая выше датаграмма предназначена для прикладной программы на этом хосте.

14. Модуль передает данные прикладной программе в ответ на системный вызов. В качестве результата этого вызова передаются адрес получателя и другие параметры.

Описание функций:

Функция или цель протокола Internet состоит в передаче датаграммы через набор объединенных компьютерных сетей.

Это осуществляется посредством передачи датаграмм от одного модуля Internet к другому до тех пор, пока не будет достигнут получатель.

Модули Internet находятся на хостах и шлюзах системы Internet. Датаграммы направляются с одного модуля Internet на другой через конкретные компьютерные сети, основанные на интерпретации Internet адресов.

Таким образом, одним из важных механизмов протокола Internet является Internet адрес. При передаче сообщений с одного Internet модуля на другой датаграммы могут нуждаться в прохождении через сети, для которых максимальный размер пакета меньше, чем размер датаграммы. Чтобы преодолеть эту сложность, в протокол Internet включен механизм фрагментации.

Адресация:

В протоколе сделано разграничение между именами, адресами и маршрутами. Имя показывает искомый нами объект. Адрес показывает его местонахождение. Internet имеет дело с адресами. Перевод имен в адреса является задачей протоколов более высокого уровня (прикладных программ или протоколов передачи синхронизации с хоста на хост). Собственно модуль Internet осуществляет отображение адресов Internet на адреса локальной сети. Создание карты адресов локальной сети для получения маршрутов - задача процедур более низкого уровня (процедур локальной сети или шлюзов). Адреса имеют фиксированную длину четыре октета (32 бита). Адрес начинается с сетевого номера, за которым следует локальный адрес (называемый полем остатка "rest"). Существуют три формата или класса адресов Internet.

В классе а самый старший бит нулевой. Следующие 7 бит определяют сеть, а последние 24 бита - локальный адрес. В классе b самые старшие два бита равны соответственно 1 и 0, следующие 14 бит определяют сеть, а последние 16 бит - локальный адрес. В классе c три самых старших бита равны соответственно 1, 1 и 0, следующие 21 бит определяют сеть, а последние 8 бит - локальный адрес. При отображении карты Internet адресов на адреса локальной сети следует соблюдать осторожность.

Единичный хост-компьютер должен уметь работать так, как если бы на его месте существовало несколько отдельных хост-компьютеров для использования нескольких адресов Internet. Некоторые хост-компьютеры будут также иметь несколько физических интерфейсов (multi-homing). Таким образом, следует обеспечить каждый хост-компьютер несколькими физическими сетевыми интерфейсами, имеющими по несколько логических адресов Internet. Примеры построения карты адресов можно найти в документе "Address Mapping".

Фрагментация. Фрагментация Internet датаграммы необходима, когда эта датаграмма возникает в локальной сети, позволяющей работать с пакетами большого размера, и затем должна пройти к получателю через другую локальную сеть, которая ограничивает пакеты меньшим размером. Internet датаграмма может быть помечена как не фрагментируемая. Любая Internet датаграмма, помеченная таким образом, не может быть фрагментирована модулем Internet ни при каких условиях. Если же Internet датаграмма, помеченная как не фрагментируемая, тем не менее не может достигнуть получателя без фрагментации, то вместо этого она будет разрушена.

Фрагментация, перенос и сборка в локальной сети, невидимые для модуля Internet протокола, называются внутрисетевой фрагментацией и могут быть всегда использованы. Необходимо, чтобы Internet процедуры фрагментации и сборки могли разбивать датаграмму на почти любое количество частей, которые впоследствии могли бы быть вновь собраны. Получатель фрагмента использует поле идентификации для того, чтобы быть убежденным в том, что фрагменты различных датаграмм не будут перепутаны.

Поле смещения фрагмента сообщает получателю положение фрагмента в исходной датаграмме. Смещение фрагмента и длина определяют кусок исходной датаграммы, принесенный этим фрагментом. Флаг "more fragments" показывает (посредством перезагрузки) появление последнего фрагмента. Эти поля дают достаточное количество информации для сборки датаграмм. Поле идентификации позволяет отличить фрагменты одной датаграммы от фрагментов другой. Модуль Internet, отправляющий Internet датаграмму, устанавливает в поле идентификации значение, которое должно быть уникальным для данной пары отправитель - получатель, а также время, в течении которого датаграмма будет активна в системе Internet. Модуль протокола, отправляющий нерасчлененную датаграмму, устанавливает в нуль флаг "more fragments" и смещение во фрагменте. Чтобы расчленить большую Internet датаграмму, модуль протокола Internet (например, шлюз), создает две новые Internet датаграммы и копирует содержимое полей Internet заголовка из большой датаграммы в оба новых Internet заголовка. Данные из старой датаграммы делятся на две части по границе на очередном восьмом октете (64 бита).

Полученная таким образом вторая часть может быть кратна 8 октетам, а может и не быть, но первая часть кратна всегда. Заказывается количество блоков первой части NFB (количество блоков фрагмента). Первая часть данных помещается в первую новую Internet датаграмму, в поле общей длины помещается длина первой датаграммы.

Флаг "more fragments" устанавливается в единицу. Вторая часть данных помещается во вторую новообразованную Internet датаграмму, в поле общей длины заносится длина второй датаграммы. В поле смещения фрагмента во второй Internet датаграмме устанавливается значение такого же поля в исходной большой датаграмме, увеличенное на NFB. Эта процедура может быть обобщена на случай многократного расщепления исходной датаграммы. Чтобы собрать фрагменты Internet датаграммы, модуль протокола Internet (например, модуль на хост-компьютере) объединяет Internet датаграммы, имеющие одинаковые значения в полях идентификатора, отправителя, получателя и протокола. Собственно объединение заключается в помещении данных из каждого фрагмента в позицию, указанную в заголовке Internet пакета в поле "fragment offset". Первый фрагмент будет иметь в поле "fragment offset" нулевое значение, а последний фрагмент будет иметь флаг "more fragments", вновь установленный в нуль.