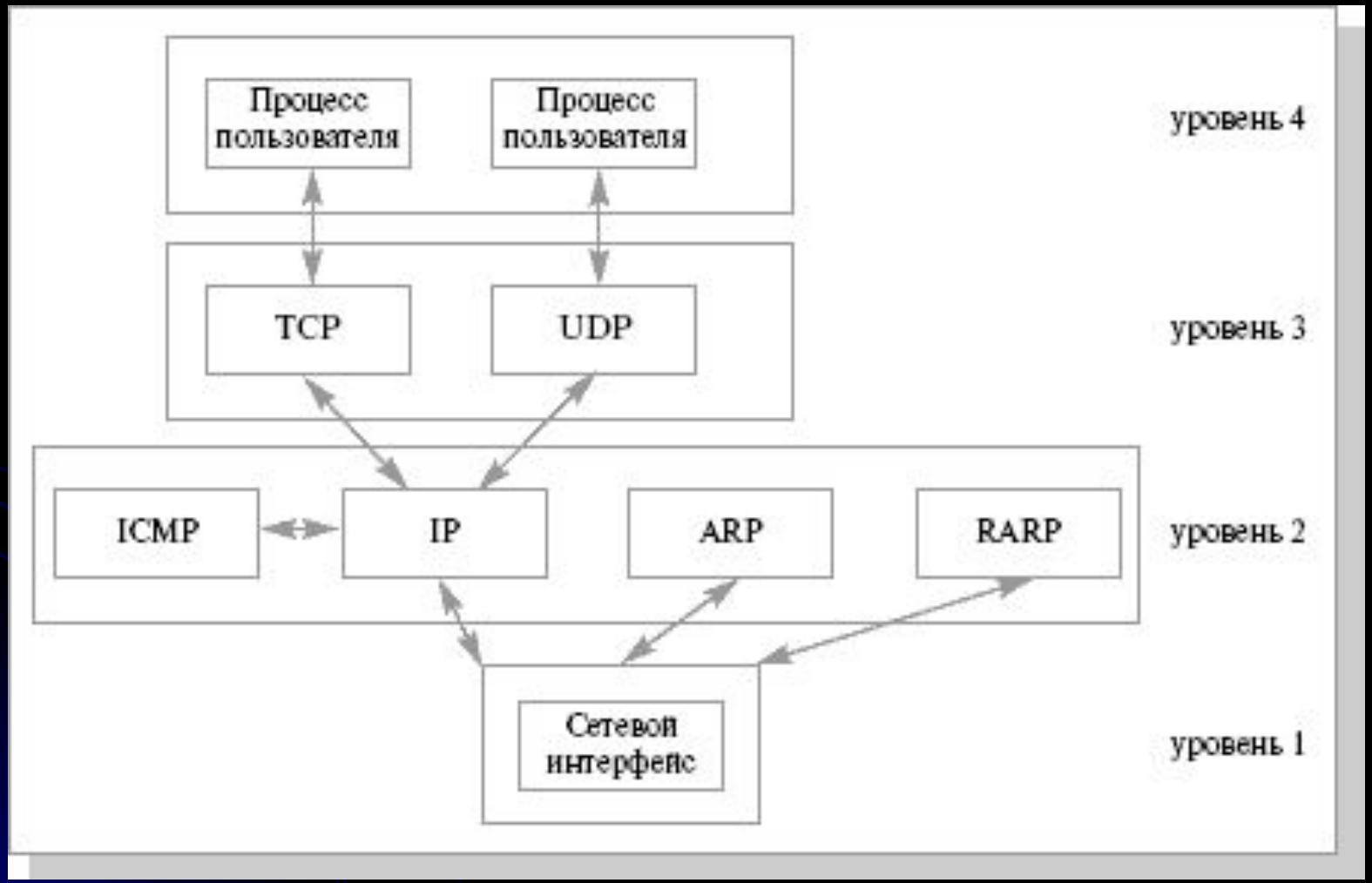
Общие сведения о TCP/IP

Уровни TCP/IP

Основные протоколы семейства



Уровень сетевого интерфейса

Уровень сетевого интерфейса составляют протоколы, которые обеспечивают передачу данных между узлами связи, физически напрямую соединенными друг с другом,

или подключенными к одному сегменту сети, и соответствующие физические средства передачи данных.

В протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet ,Fast Ethernet, 100VG-AnyLAN,

для глобальных сетей - протоколы соединений "точка-точка" SLIP(Serial Line Internet Protocol) и PPP(PPP — это механизм для создания и запуска IPдля глобальных сетей - протоколы соединений "точка-точка" SLIP(Serial Line Internet Protocol) и PPP(PPP — это механизм для создания и запуска IP (Internet Protocol) и других сетевых протоколов на последовательных линиях связи , протоколы территориальных сетей с коммутацией пакетов X.25

физические средства : витая пара, коаксиальный кабель, оптоволоконный кабель и т.д.

Протокол SLIP (Serial Line Internet Protocol).

- протокол применяют как на выделенных, так и на коммутируемых линиях связи со скоростями от 1200 до 19200 бит в секунду
- В отличии от Ethernet, SLIP не "заворачивает" IP-пакет в свою обертку, а "нарезает" его на "кусочки", каждый из которых начинается символом ESC, а кончается символом END.
- SLIP не позволяет выполнять какие-либо действия, связанные с адресами, т.к. в структуре пакета не предусмотрено поле адреса и его специальная обработка. Компьютеры, взаимодействующие по SLIP, обязаны знать свои IP-адреса заранее.
- SLIP не позволяет различать пакеты по типу протокола, например, IP или DECnet.
- В SLIP нет информации, позволяющей корректировать ошибки линии связи. Коррекция ошибок возлагается на протоколы транспортного уровня - TCP, UDP.

Протокол PPP (Point to Point Protocol)

- назначение - управление передачей данных по выделенным или коммутируемым линиям связи.
- PPP обеспечивает стандартный метод взаимодействия двух узлов сети. Предполагается, что обеспечивается двунаправленная одновременная передача данных.
- В отличии от SLIP, PPP позволяет одновременно передавать по линии связи пакеты различных протоколов.

PPP состоит из трех частей:

- механизма инкапсуляции (encapsulation),
- протокола управления соединением (link control protocol) и
- семейства протоколов управления сетью (network control protocols).

Уровень Internet. Протоколы IP, ICMP, ARP, RARP. Internet–адреса

Уровень Internet обеспечивает доставку информации от сетевого узла отправителя к сетевому узлу получателя без установления *виртуального соединения* с помощью *датаграмм* и не является надежным.

Центральным протоколом уровня является *протокол IP*. Вся информация, поступающая к нему от других протоколов, оформляется в виде IP-пакетов данных (IP datagrams).

- ***IP – Internet Protocol***. Это протокол, который обеспечивает доставку пакетов информации для *протокола ICMP* и протоколов *транспортного уровня* TCP и UDP.
- ***ARP*** – Address Resolution Protocol. Это протокол для отображения адресов *уровня Internet* в адреса *уровня сетевого интерфейса*.
- ***RARP*** – Reverse Address Resolution Protocol. Этот протокол служит для решения обратной задачи: отображения адресов *уровня сетевого интерфейса* в адреса *уровня Internet*.
- ***ICMP*** – Internet Control Message Protocol. Протокол обработки ошибок и обмена управляющей информацией между узлами сети.

Функции IP

- определение пакета, который является базовым понятием и единицей передачи данных в сети Internet;
- определение адресной схемы, которая используется в сети Internet;
- передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем (другими словами мультиплексирование транспортных датаграмм во фреймы канального уровня);
- маршрутизация пакетов по сети, т.е. передача пакетов от одного шлюза к другому с целью передачи пакета машине-получателю;
- "нарезка" и сборка из фрагментов пакетов транспортного уровня.

IP

Каждый IP-пакет может передаваться по сети независимо от других пакетов и, возможно, по своему собственному маршруту.

IP вычисляет и проверяет контрольную сумму, которая покрывает только его собственный 20-байтовый заголовок для пакета информации.

IP-уровень *семейства TCP/IP* не обеспечивает надежную связь, не гарантирует доставку отправленного пакета информации и что пакет будет доставлен без ошибок.

Если IP-заголовок пакета при передаче оказывается испорченным, то весь пакет просто отбрасывается. Ответственность за повторную передачу пакета тем самым возлагается на вышестоящие уровни.

IP (далее)

IP протокол, при необходимости, осуществляет фрагментацию и дефрагментацию данных, передаваемых по сети.

Если размер IP-пакета слишком велик для дальнейшей передачи по сети, то полученный пакет разбивается на несколько фрагментов, и каждый фрагмент оформляется в виде нового IP-пакета с теми же адресами отправителя и получателя.

Фрагменты собираются в единое целое только в конечной точке своего путешествия. Если при дефрагментации пакета обнаруживается, что хотя бы один из фрагментов был потерян или отброшен, то отбрасывается и весь пакет целиком.

IPv4

IP четвёртой версии, IPv4. Каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (или «байта», подразумевая распространённый восьмибитовый минимальный адресуемый фрагмент памяти ЭВМ).

Компьютеры в подсетях объединяются общими начальными битами адреса.

Количество бит, общее для данной подсети, называется маской подсетиКоличество бит, общее для данной подсети, называется маской подсети (ранее использовалось деление пространства адресов по классам — A, B, C; класс сети определялся диапазоном значений старшего октета и определял число адресуемых узлов в данной сети, сейчас используется бесклассовая адресация).

IP-пакет (структура)

IP-пакет — форматированный блок информации, передаваемый по вычислительной сети. При использовании пакетного форматирования сеть может передавать длинные сообщения более надежно и эффективно.

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Версия				IHL				Тип обслуживания								Длина пакета															
Идентификатор																Флаги				Смещение фрагмента											
Число переходов (TTL)								Протокол								Контрольная сумма заголовка															
IP-адрес отправителя (32 бита)																															
IP-адрес получателя (32 бита)																															
Параметры (до 320 бит)																Данные (до 65535 байт минус заголовок)															

Классы

IP-адреса делятся на пять классов – A, B, C, D и E.

Для коммерческого использования предназначены только первые 3.

Класс	*Маска*	*Количество битов, сеть/хост*	*Максимально количество хостов*
A	255.0.0.0	8 бит на сеть/24 бита на хост	16777214 (2^{24}-2)*
B	255.255.0.0	16 бит на сеть/16 бит на хост	65534 (2^{16}-2)
C	255.255.255.0	24 бит на сеть/8 бит на хост	254 (2^{8}-2)

Класс	*Диапазон*
A	10.0.0.0 – 10.255.255.255 (255 сетей класса A)
B	172.16.0.0 – 172.31.255.255 (31 сеть класса B)
C	192.168.0.0 – 192.168.255.255 (255 сетей класса C)

Маска подсети

Маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

Биты маски, установленные в 1
определяют сеть, а в 0 – хост.

Наример:
192.168.2.31/255.255.255.0
Маска подсети 255.255.255.0 в двоичном виде будет выглядеть:
1111111 1111111 1111111 00000000
Отсюда можно сделать вывод, что для того чтобы найти адрес 192.168.2.31 нужно найти
сеть 192.168.2.0, а в ней хост 31.

Бесклассовая адресация

Иногда встречается запись IP-адресов вида 10.96.0.0/11. Данный вид записи заменяет собой указание диапазона IP-адресов. Число после слэша означает количество единичных разрядов в маске подсети.

Для приведённого примера маска подсети будет иметь двоичный вид 11111111 11100000 00000000 00000000 или то же самое в десятичном виде: 255.224.0.0.

11 разрядов IP-адреса отводятся под номер сети, а остальные 32 - 11 = 21 разрядов полного адреса — под локальный адрес в этой сети. Итого, 10.96.0.0/11 означает диапазон адресов от 10.96.0.0 до 10.127.255.255

IPv6

В этом протоколе адрес имеет длину 128 бит. Изначально столь длинные адреса вводились для того, чтобы решить проблему сокращения адресного пространства IPv4.

С внедрением стандарта IPv6 IP-адреса стали группироваться в кластеры вокруг провайдеров Internet. Граница между сетевой и машинной частями адреса в IPv6 зафиксирована на отметке 64 бита. В сетевой части адреса граница между блоками общей и локальной топологии также зафиксирована и проходит на отметке 48 битов.

Тип адреса	Префикс провайдера	Подсеть	Идентификатор узла
3 бита	45 битов	16 битов	64 бита

В IPv6 MAC-адреса видны на уровне IP. Тип и модель сетевой платы кодируются в первой половине MAC-адреса, что облегчает задачу хакерам.

Маршрутизация

Маршрутизация- процесс направления пакета по лабиринту сетей, находящихся между отправителем и адресатом.

Данные маршрутизации в системе TCP/IP имеют форму правил (маршрутов). Данные маршрутизации хранятся в одной из таблиц ядра. Любой элемент подобной таблицы содержит несколько параметров, включая сетевую маску для каждой перечисленной сети.

Для направления пакета по конкретному адресу ядро подбирает наиболее подходящий маршрут (т.е. тот, где самая длинная маска). Если ни одни из маршрутов (в том числе стандартный) не подходят, то отправителю возвращается ICMP сообщение об ошибке «network unreachable».

Таблица маршрутизации

Можно посмотреть с помощью команды netstat –r или route get

student@student-desktop:~$ netstat –r
Таблица маршутизации ядра протокола IP
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.1.0 * 255.255.255.0 U 0 0 0 eth0
В рассматриваемой системе одна сетевая плата 192.168.1.0 (eth0)

Вести таблицы маршрутизации можно статически и динамически или комбинированным методом.

Статический маршрут – это маршрут, который задается явно с помощью команды route. Он должен оставаться в таблице маршрутизации на всем протяжении работы системы. Во многих случаях такие маршруты задаются с помощью одного из стартовых сценариев во время начального запуска системы.

Динамическая маршрутизация выполняется процессом-демоном, который ведет и модифицирует таблицу маршрутизации.

Адресация в IP-сетях

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

1. Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта, например, 08-00-10-3D-BC-01

Префикс	Производитель	Префикс	Производитель
00:00:0C	Cisco	08:00:0B	Unisys
00:00:0F	NeXT	08:00:10	T&T
00:00:10	Sytek8:00:11	Tektronix	
00:00:1D	Cabletron	08:00:14	Exelan
00:00:65	Network General	08:00:1A	Data General
00:00:6B	MIPS	08:00:1B	Data General

Адресация в IP-сетях

2. IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов.
3. DNS. Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Используется на прикладном уровне, например, в протоколах FTP или telnet.

Протокол ARP (RFC 826)

- *Address Resolution Protocol* используется для определения соответствия IP-адреса адресу Ethernet.
- Протокол используется в локальных сетях. Отображение осуществляется только в момент отправления IP-пакетов, так как только в этот момент создаются заголовки IP и Ethernet.
- Отображение адресов осуществляется путем поиска в ARP-таблице.

ARP

- *Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос,*
- *вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес,*
- *рассылает запрос широковещательно.*
- *Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным.*
- *В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.*
- *ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети.*

ARP

формат пакета протокола ARP для передачи по сети Ethernet.

Тип сети		*Тип протокола*
Длина локального адреса	*Длина сетевого адреса*	*Операция*
Локальный адрес отправителя (байты 0 - 3)		
Локальный адрес отправителя (байты 4 - 5)		*IP-адрес отправителя (байты 0-1)*
IP-адрес отправителя (байты 2-3)		*Искомый локальный адрес (байты 0 - 1)*
Искомый локальный адрес (байты 2-5)		
Искомый IP-адрес (байты 0 - 3)		

ARP-таблица состоит из двух столбцов:

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

- В первом столбце содержится IP-адрес, а во втором Ethernet-адрес.
- Таблица соответствия необходима, так как адреса выбираются произвольно и нет какого-либо алгоритма для их вычисления.
- Если машина перемещается в другой сегмент сети, то ее ARP-таблица должна быть изменена.

DNS (Domain Name System)

- *Протокол DNS является служебным протоколом прикладного уровня*
- DNS (Domain Name System) - *распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.*
- *Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла.*
- *Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.*

DNS

- *Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.*

- *Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу.*

- *Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet.*

DNS

- *База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.*
- *Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.*
- *Корень базы данных DNS управляется центром Internet Network Information Center.*
- *Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166.*

DNS

- *Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:*
- *com - коммерческие организации (например, microsoft.com);*
- *edu - образовательные (например, mit.edu);*
- *gov - правительственные организации (например, nsf.gov);*
- *org - некоммерческие организации (например, fidonet.org);*
- *net - организации, поддерживающие сети (например, nsf.net).*

Прочие протоколы сетевого уровня

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.

ICMP

Протокол ICMP не делает протокол IPПротокол ICMP не делает протокол IP средством надёжной доставки сообщений. Для этих целей существует TCP.

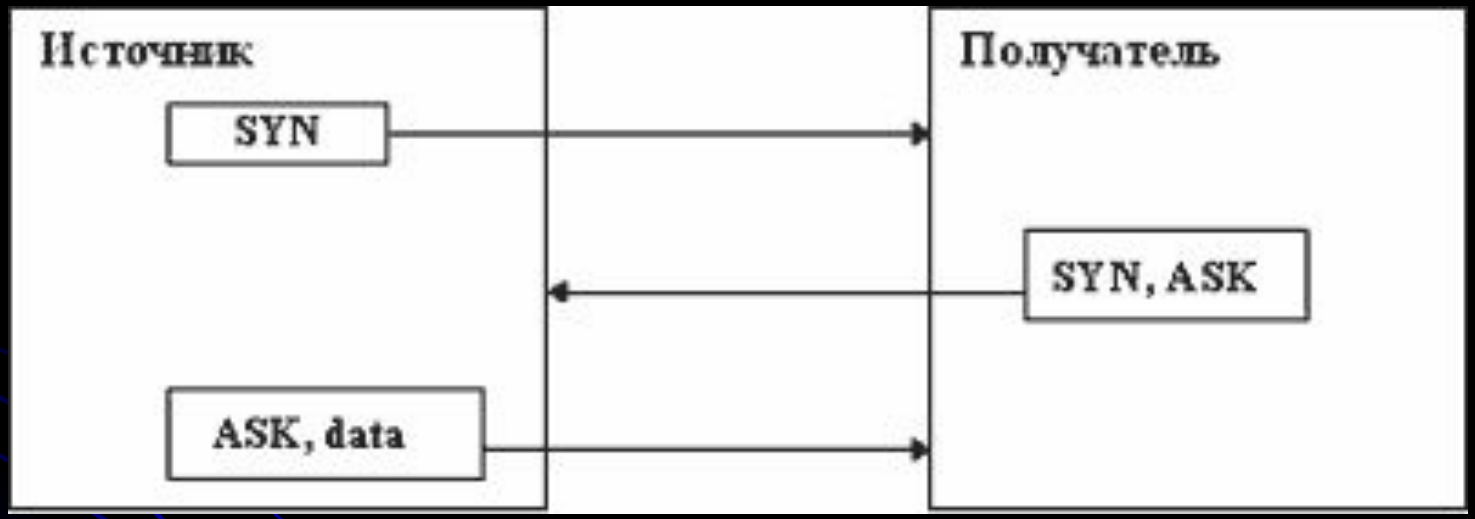
- ICMP сообщения (тип 12) генерируются при нахождении ошибок в заголовке IP пакета (за исключением самих ICMP пакетов, дабы не привести к бесконечно растущему потоку ICMP сообщений об ICMP сообщениях).
- ICMP сообщения (тип 3) генерируются маршрутизатором при отсутствии маршрута к адресату.
- Утилита ping, служащая для проверки возможности доставки IP пакетов использует ICMP сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ).
- ICMP сообщения с типом 5 используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя.

Транспортный уровень

Протокол TCP реализует потоковую модель передачи информации. Он представляет собой ориентированный на установление логической связи (connection-oriented), надежный дуплексный способ связи между процессами в сети.

Протокол UDP, наоборот, является способом связи ненадежным, ориентированным на передачу сообщений (*датаграмм*). От *протокола IP* он отличается двумя основными чертами: использованием для проверки правильности принятого сообщения контрольной суммы, насчитанной по всему сообщению, и передачей информации не от узла сети к другому узлу, а от отправителя к получателю.

Установка соединения TCP



Сокеты

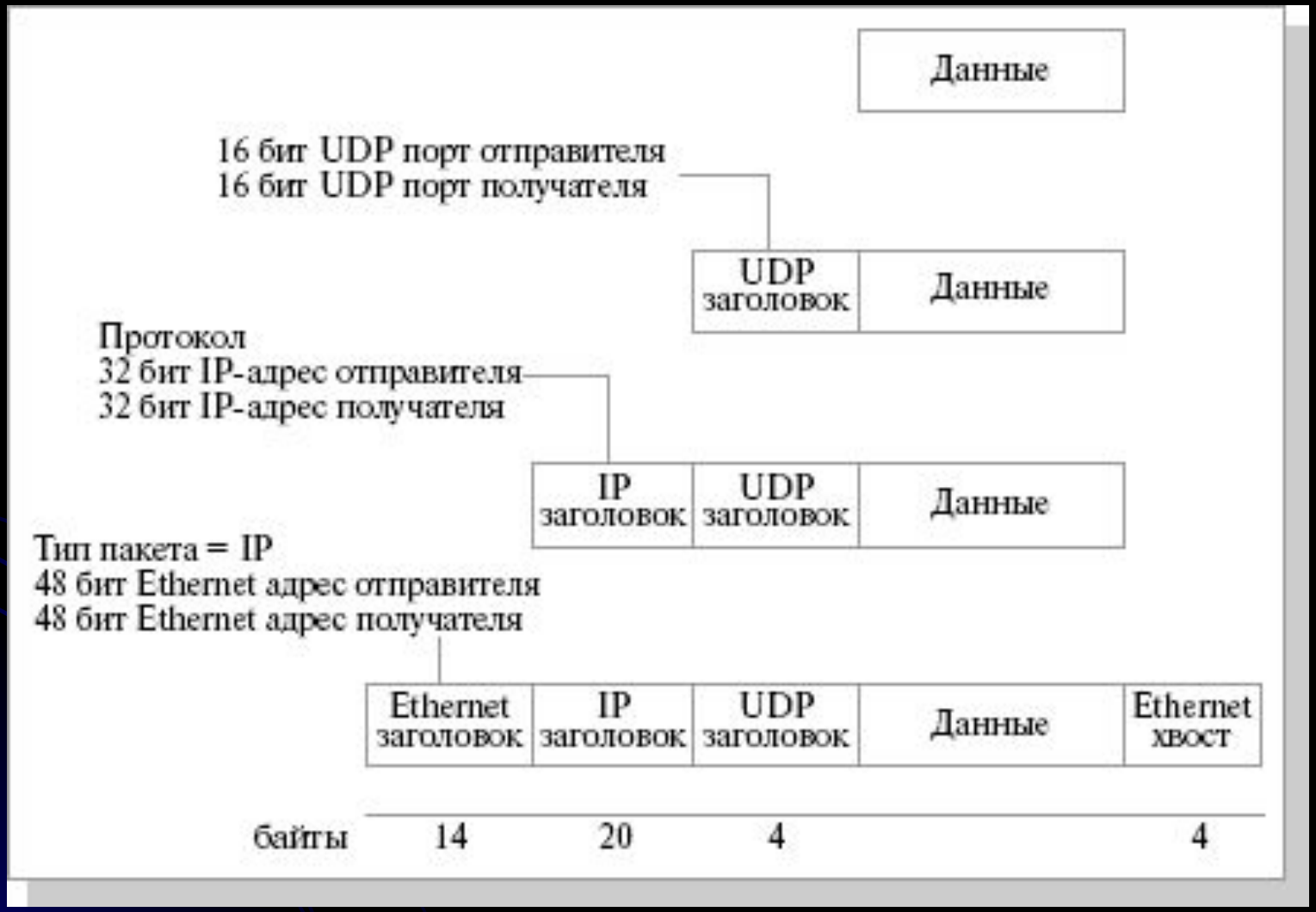
- Полный адрес удаленного процесса или промежуточного объекта для конкретного способа связи с точки зрения операционных систем определяется парой адресов: <числовой адрес компьютера в сети, локальный адрес>.
- Такая пара получила название socket (гнездо, панель), так как по сути дела является виртуальным коммуникационным узлом ведущим от объекта во внешний мир и наоборот.
- При непрямой адресации сами промежуточные объекты для организации взаимодействия процессов также именуются *сокетами*.

TCP/IP

Семейство протоколов TCP/IP имеет иерархическую систему адресации, которая включает в себя несколько уровней:

- Физический пакет данных, передаваемый по сети, содержит физические адреса узлов сети (*MAC-адреса*) с указанием на то, какой протокол *уровня Internet* должен использоваться для обработки передаваемых данных.
- IP-пакет данных содержит 32-битовые *IP-адреса* компьютера-отправителя и компьютера-получателя, и указание на то, какой вышележащий протокол (TCP, *UDP* или еще что-нибудь) должен использоваться для их дальнейшей обработки.
- Служебная информация транспортных протоколов (UDP-заголовок к данным и TCP-заголовок к данным) должна содержать 16-битовые номера *портов* для *сокета* отправителя и сокета получателя.

Инкапсуляция



Уровень приложений/процессов

К этому уровню можно отнести протоколы:

FTP (File Transfer Protocol),

TFTP(Trivial File Transfer Protocol),

telnet,

SMTP (Simple Mail Transfer Protocol) и другие, которые поддерживаются соответствующими системными утилитами.

FTP (File Transfer Protocol)

- Протокол пересылки файлов реализует удаленный доступ к файлу.

- Чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP.

- FTP выполняет аутентификацию пользователей.
- 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.

TFTP

Trivial File Transfer Protocol

- протокол реализует только передачу файлов,
- в качестве транспорта используется протокол без установления соединения - UDP.

telnet

- Протокол 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.

SNMP

Simple Network Management Protocol используется для организации сетевого управления.

Изначально протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet

С ростом популярности протокол SNMP стали применять и для управления любым коммуникационным оборудованием - концентраторами, мостами, сетевыми адаптерами и т.д. и т.п.