

ВМСИС

Лекция 7

Введение в вычислительные сети

Причины и история возникновения компьютерных сетей

- 60-е Создание первых мейнфреймов
 - Возникает необходимость перераспределения вычислительной нагрузки
 - Доступ к мейнфреймам с терминалов удаленных на десятки километров
 - Используются существующие телекоммуникационные сети
- 70-е Инициатива по созданию ARPANET
 - Необходимо обмениваться информацией между машинами распределенными по всей стране
 - Разрабатывается стандарт стека протоколов обеспечивающий обмен данными между различными типами машин и различными операционными системами
 - Появление небольших ЭВМ вызывает потребность в организации ЛВС
 - Первые версии стека TCP/IP
- 80-е Появление персональных ЭВМ
 - Необходимо объединять сотни ЭВМ в локальные сети и обеспечивать доступ к удаленным машинам
 - Стандартизируются протоколы ЛВС - Ethernet, Token Ring
 - Появляются стандарты протоколов верхнего уровня POP, SMTP, FTP и т.д.

История развития компьютерных сетей

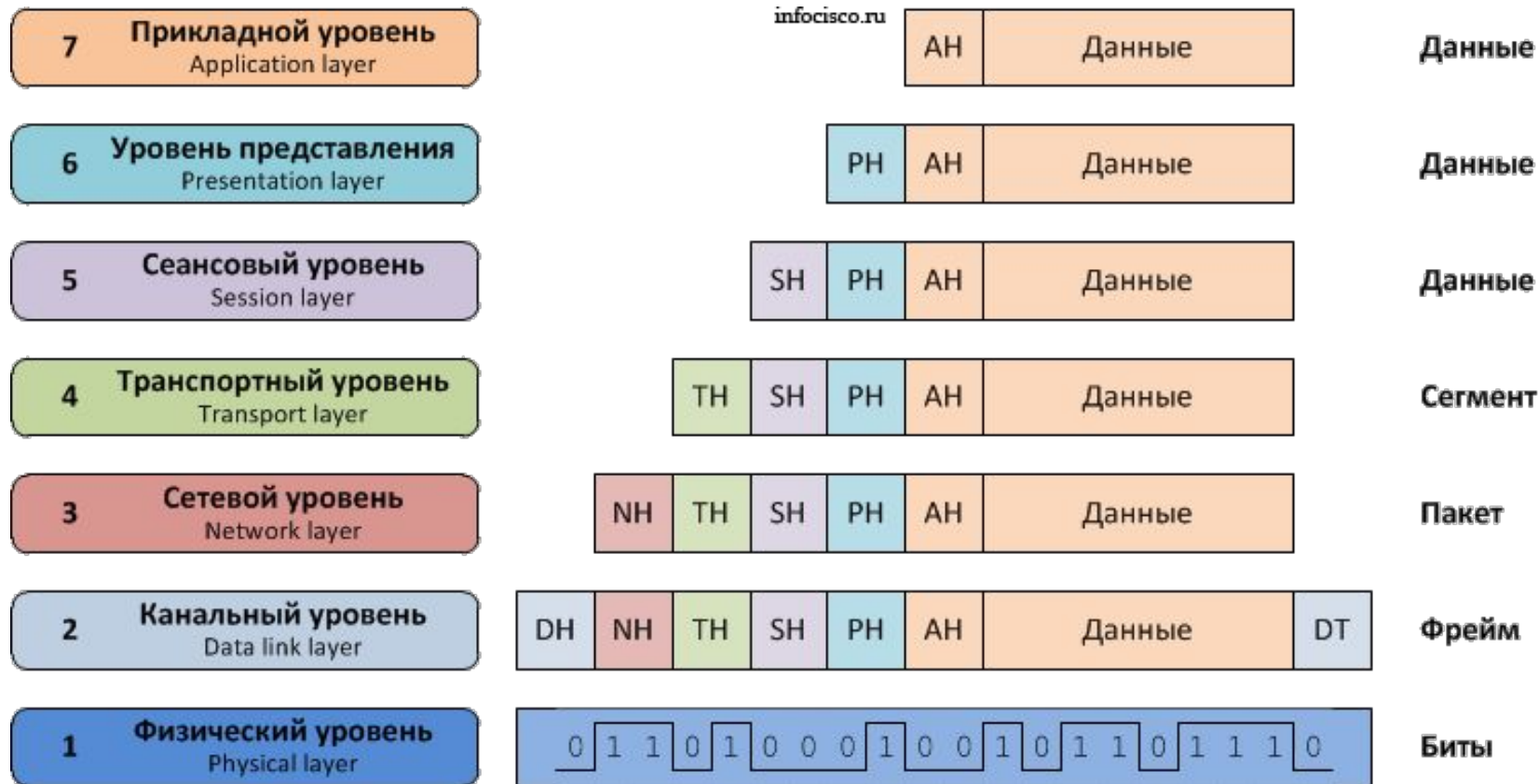
- 90-е Зарождение и развитие Internet и WWW
 - ARPANET выходит за рамки военного применения
 - 1992 - первый драфт протокола HTTP, появление браузера MOSAIC
 - Активно развивается модемный доступ в сеть
- 00-е Появление Web 2.0
 - Все вычислительные системы получают доступ в общую сеть
 - Объем передаваемых данных увеличивается в тысячи раз
- 10-е Повсеместное развитие беспроводного доступа
 - Появление стандартов 3G/4G/5G
 - Все современные города покрыты сетью WiFi/4G
 - Интернет вещей

Сетевая модель ISO OSI

Open system interconnection basic reference model

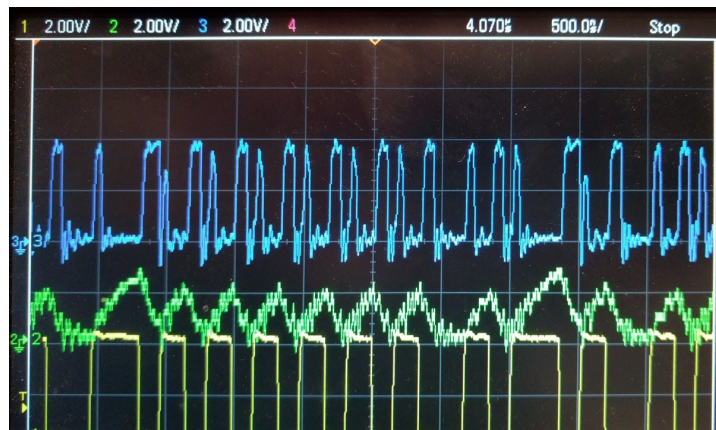
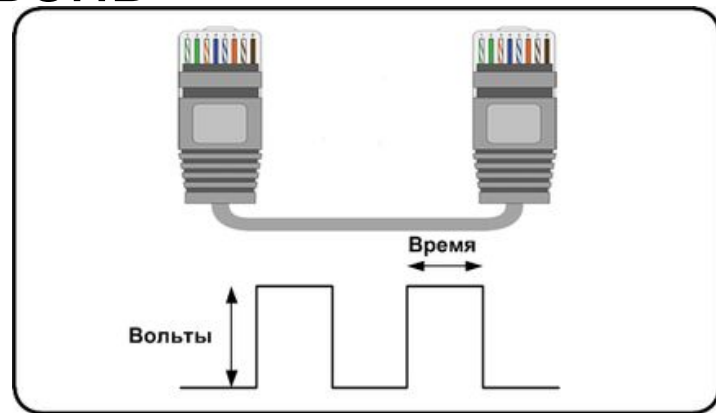
- Планировалась и разрабатывалась с конца 70-х с целью стандартизации архитектуры сетевого взаимодействия
- Описывает 7 уровней ВС от физического, до уровня приложения
- Не используется в чистом виде

Уровни модели OSI



Physical layer - физический уровень

- Определяет среду передачи данных
 - Медный провод
 - Оптоволокно
 - Радиоволны
- Физические характеристики сигнала
 - Уровни напряжения
 - Тип кодирования
 - Скорость передачи сигнала
- Разъемы и назначения контактов



Data link layer - канальный уровень

- Обнаружение коллизий
 - Арбитраж доступа к среде
 - Группировка бит в кадры
 - Обнаружение и исправление ошибок передачи данных
-
- Ethernet
 - Token ring
 - 802.11 (WiFi)

Коллизии

Возникают при попытке двух или более узлов осуществить передачу данных в **общей среде передачи**

Алгоритмы избежания коллизий:

- Ethernet - Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- WiFi - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

CSMA/CD

Этап 1. Узел 1 и Узел 2 хотят передать данные и прослушивают линию



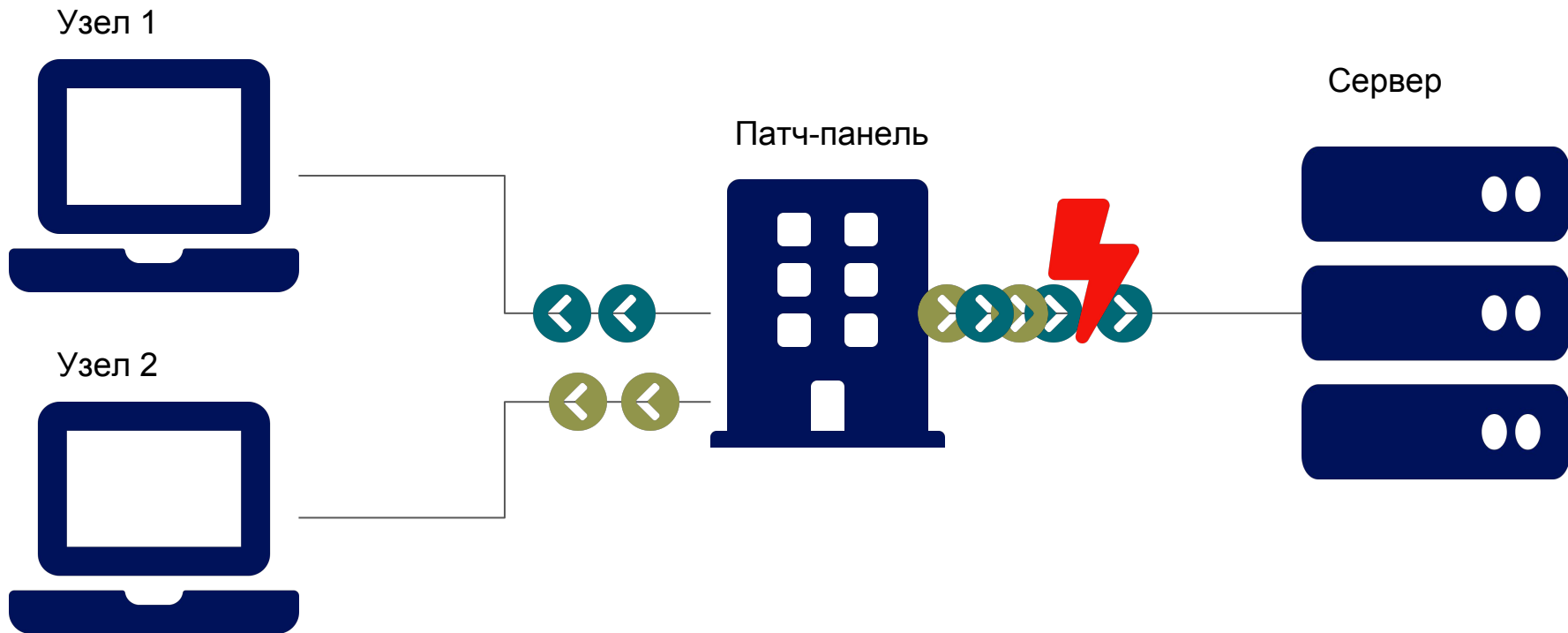
CSMA/CD

Этап 2. Линия свободна и оба узла начинают передачу



CSMA/CD

Этап 3. Попадая в одну среду сигналы накладываются друг на друга




CSMA/CD

Этап 4. Оба узла продолжают прослушивать канал. Узел 1 обнаруживает, что его сигналу что-то мешает



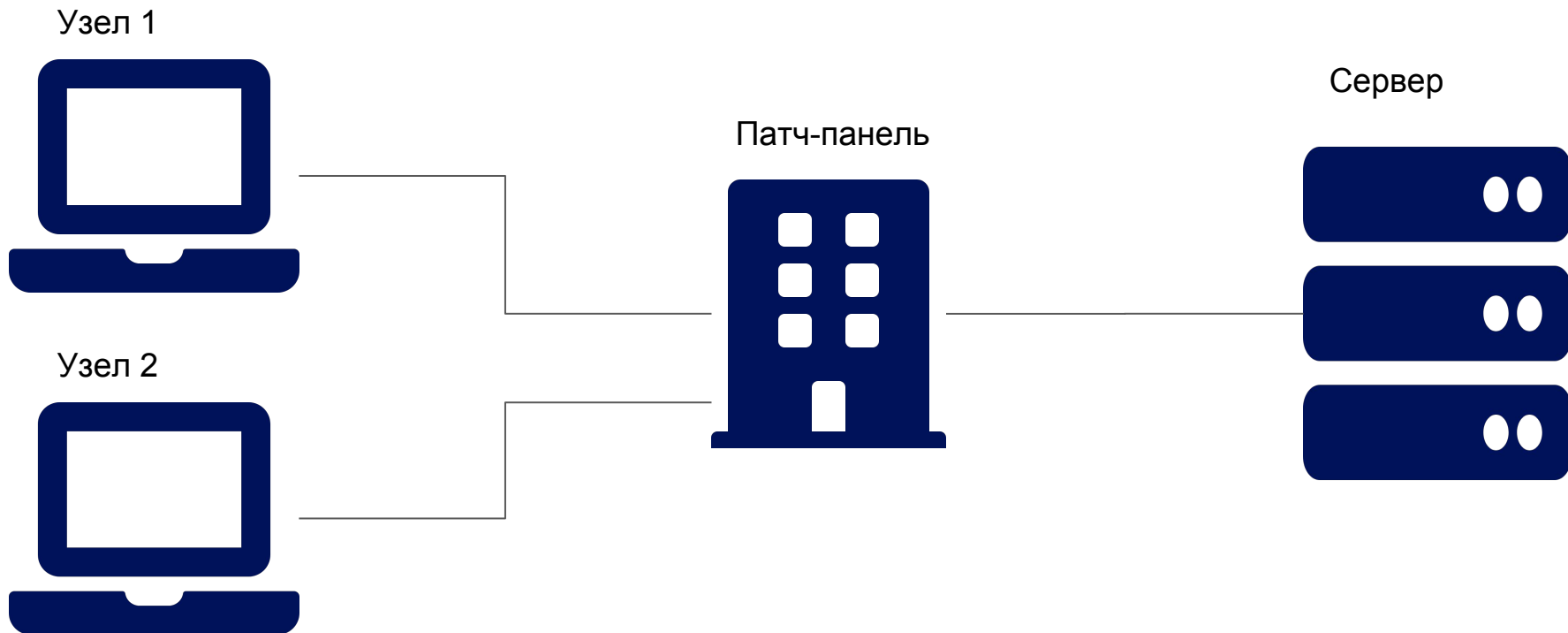
CSMA/CD

Этап 5. Для облегчения обнаружения коллизии другими узлами, Узел 1 отправляет JAM сигнал 



CSMA/CD

Этап 6. Все узлы поняли, что произошла коллизия
и прервали передачу данных



CSMA/CD

Этап 7. Все узлы желающие передать данные
ожидают случайный промежуток времени



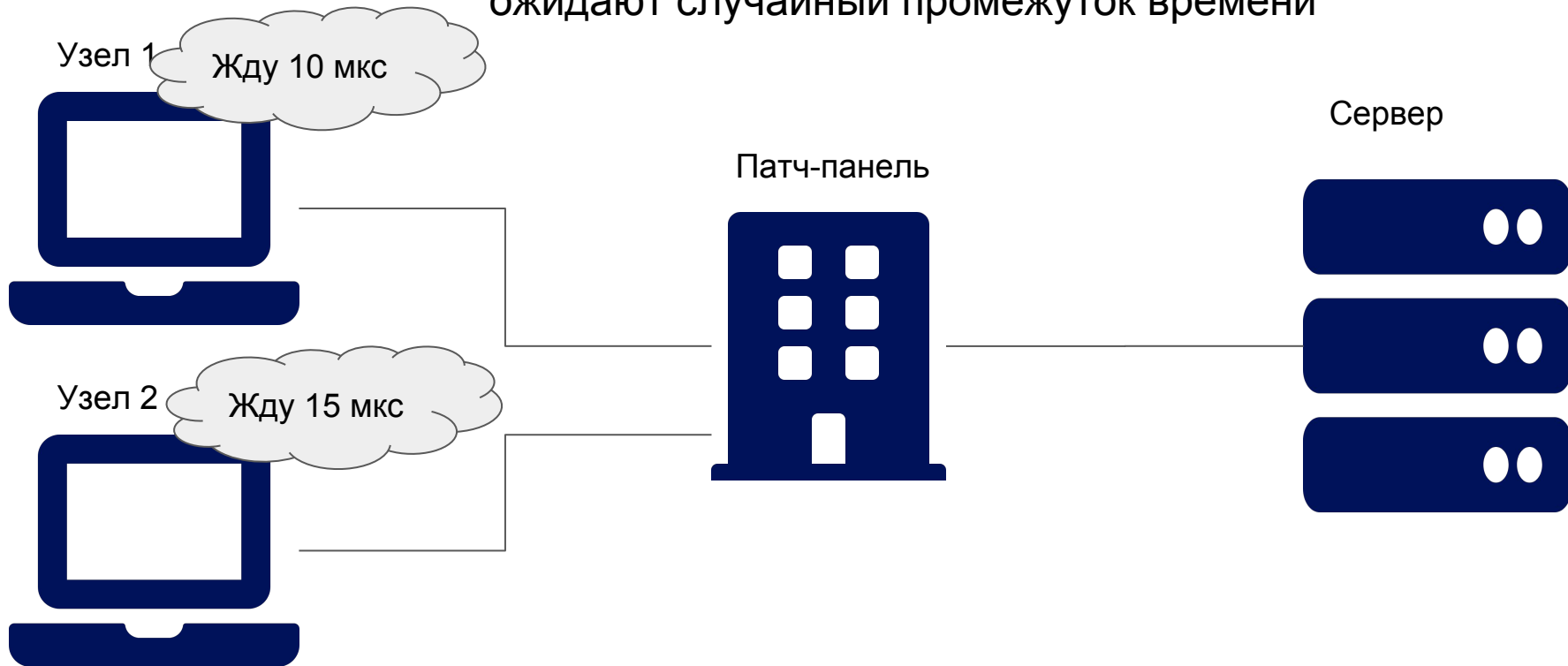
CSMA/CD

Этап 8. Узел 1 первым начинает передачу, а Узел 2 обнаруживает занятость канала и ждет



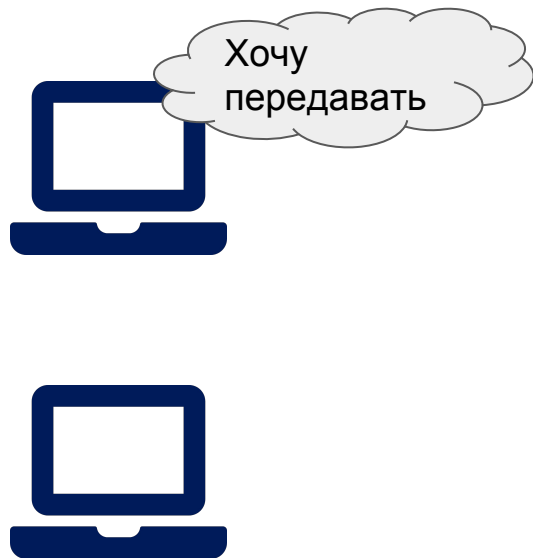
CSMA/CD

Этап 7. Все узлы желающие передать данные
ожидают случайный промежуток времени



CSMA/CA

Этап 1. Все узлы имеющие данные для передачи прослушивают эфир



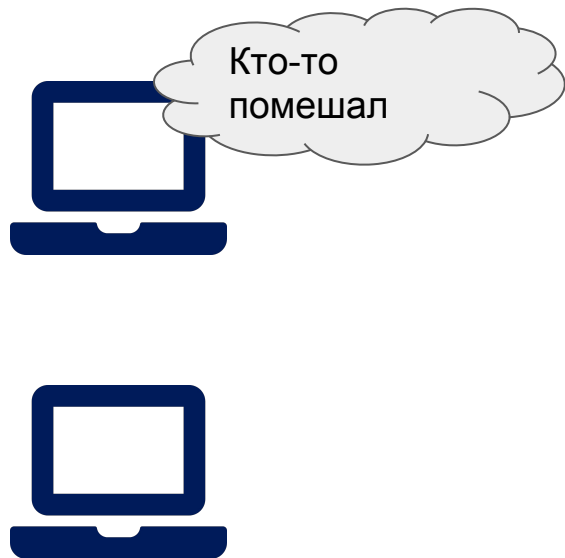
CSMA/CA

Этап 2. Если в эфире не обнаружено несущей, то передающий узел отправляет JAM пакет



CSMA/CA

Этап 3.А. В случае одновременной выдачи JAM двумя или более узлами, ситуация разрешается аналогично CSMA/CD



CSMA/CA

Этап 3.Б. Если только один пакет выдал JAM, то все остальные узлы ожидают его пакета с данными



Адресация на канальном уровне

В большинстве распространенных протоколов для адресации используются MAC-адреса.

Диапазоны адресов выдаются производителям оборудования диапазонами по 2^{24} адресов

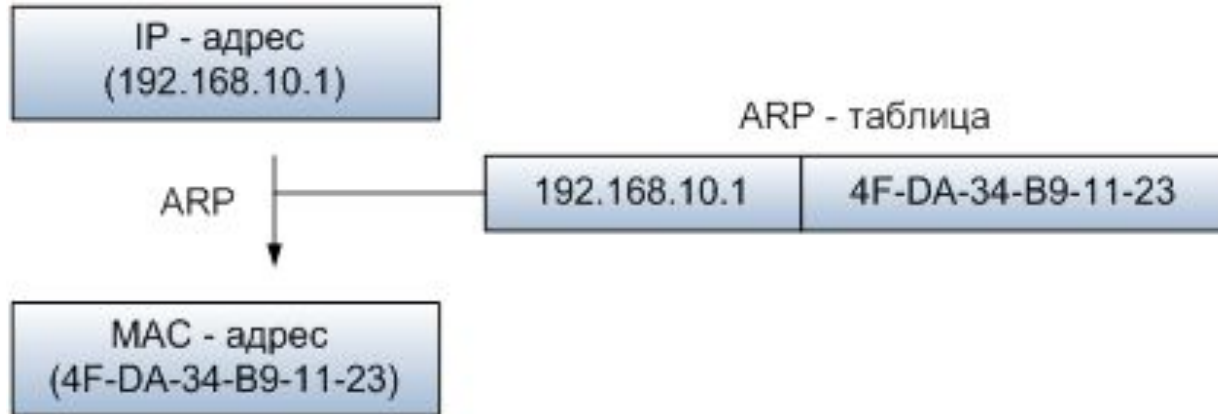
Пример: MAC адрес **bc:5f:f4:45:a3:eb**

bc:5f:f4 - ASRock Incorporation

45:a3:eb - Уникальный адрес для оборудования ASRock

Address resolution protocol - ARP

Для связи протоколов нижнего и верхнего уровней используются так называемые ARP таблицы, или таблицы соответствия логических IP адресов и адресов канального уровня



Network layer - сетевой уровень

- Присвоение сетевых адресов узлам
- Связь сетевых адресов с физическими
- Маршрутизация сообщений

- IPv4/IPv6
- IPX
- ICMP
- IGMP
- RIP

Internet Protocol ver. 4 - IPv4

- Используется для инкапсуляции протоколов транспортного уровня (UDP/TCP)
- Отвечает за маршрутизацию данных в интернете
- Не осуществляет контроль за доставкой и целостностью пакетов

Формат пакета IPv4

Биты	0-3	4-7	8-15	16-31
0-31	Версия	IHL	Тип обслуж.	Длина пакета
32-63	Идентификатор			Флаги + Смещение сегмента
64-95	TTL		Протокол	Контрольная сумма заголовка
96-127	Адрес отправителя			
128-159	Адрес получателя			
160-191	Параметры			
192-...	Данные			

Адресация IPv4

IP-адрес в протоколе IPv4 имеет размер 4 байта и состоит из двух частей

- Адрес сети
- Адрес узла в этой сети

В зависимости от назначения и максимально допустимого количества узлов в сети, их делят на 5 классов:

- Класс А - 16 777 216 узлов
- Класс В - 65 536 узлов
- Класс С - 256 узлов
- Класс D - multicast или ограниченный широковещательный адрес
- Класс Е - зарезервирован и не используется

Адресация IPv4

Примеры IP адресов:

- 192.168.22.10
 - Адрес сети: 192.168.22.0, сеть класса C
 - Адрес узла: 10
- 82.179.190.60
 - Адрес сети: 82.0.0.0, Сеть класса A

Внеклассовая адресация, использование масок

Разделение сетей по классовому признаку оказалось неэффективным. Был добавлен механизм более тонкого деления диапазонов при помощи масок.

Маска - это последовательность 1 и 0 длиной 32 бита.

Маски стандартных классов:

- Класс А: 11111111.00000000.00000000.00000000 - 255.0.0.0
- Класс В: 11111111.11111111.00000000.00000000 - 255.255.0.0
- Класс С: 11111111.11111111.11111111.00000000 - 255.255.255.0

Расчет адреса сети и адреса узла с помощью маски

IP-адрес	129.64.134.5	10000001. 01000000. 10000110. 00000101
Маска	255.255.128.0	11111111. 11111111. 10000000. 00000000

По классовой системе: Сеть 129.64.0.0, узел: 0.0.134.5

Используя маску:

	10000001.01000000.10000110.00000101
&	11111111.11111111.10000000.00000000
	<hr/>
	10000001.01000000.10000000.00000000

Сеть: 129.64.128.0, узел 0.0.6.5

Особые адреса

- **0.0.0.0** - шлюз по умолчанию
- **255.255.255.255** - широковещательный адрес по сети отправителя
- **АдресСети.ВсеЕдиницы** - широковещательный адрес по указанной сети
- **127.x.x.x** - loopback адрес
-

Диапазоны локальных сетей

- **10.x.x.x** - подсеть класса А
- **172.16.x.x** - подсеть класса В
- **192.168.x.x** - подсеть класса С
- **169.254.x.x** - link local, подсеть для автоконфигурации устройства

Маршрутизация в IP сетях

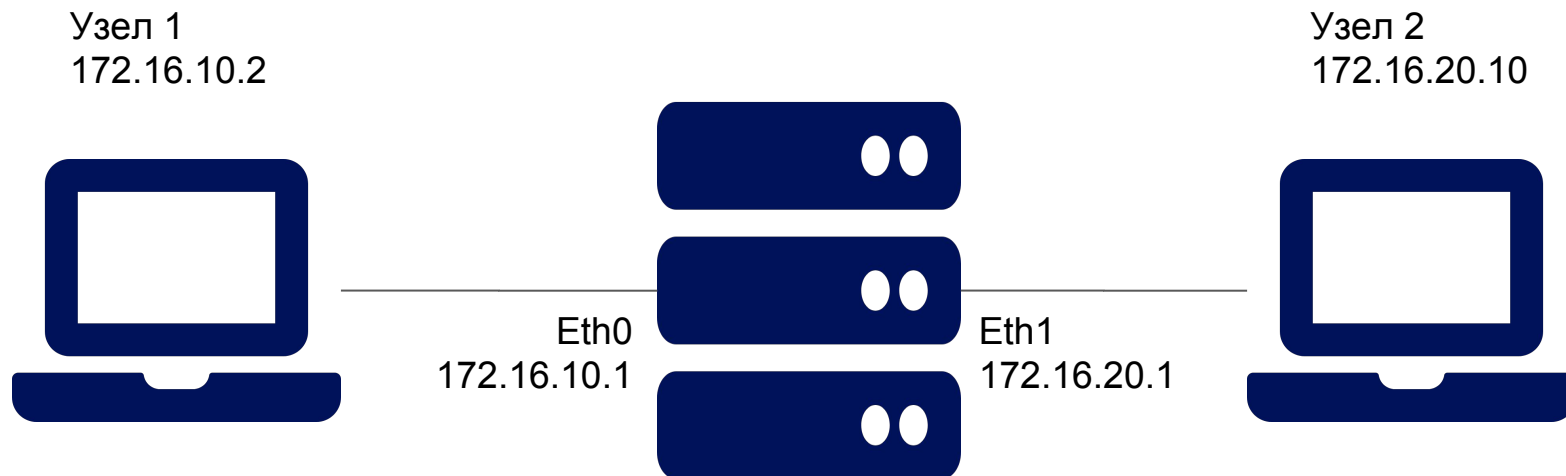
Все узлы в Интернет объединяются в одну сеть при помощи Маршрутизаторов (Router)

Для успешной маршрутизации пакета, маршрутизатор должен:

- Знать адрес назначения пакета (соответственно, знать его сеть)
- Иметь прямой доступ к сети назначения **или**
- Иметь доступ к соседнему маршрутизатору, который может передать пакет в сеть назначения

Пример маршрутизации пакета

Узел 1 отправляет команду
ping 172.16.20.2



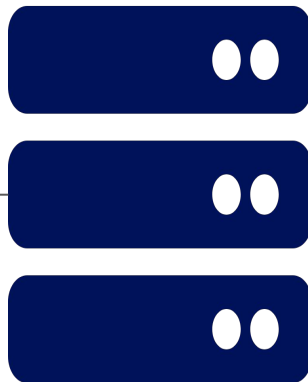
Пример маршрутизации пакета

IP определяет, что 172.16.20.2 находится в другой сети, значит нужно отправлять на маршрутизатор

Узел 1
172.16.10.2



Eth0
172.16.10.1



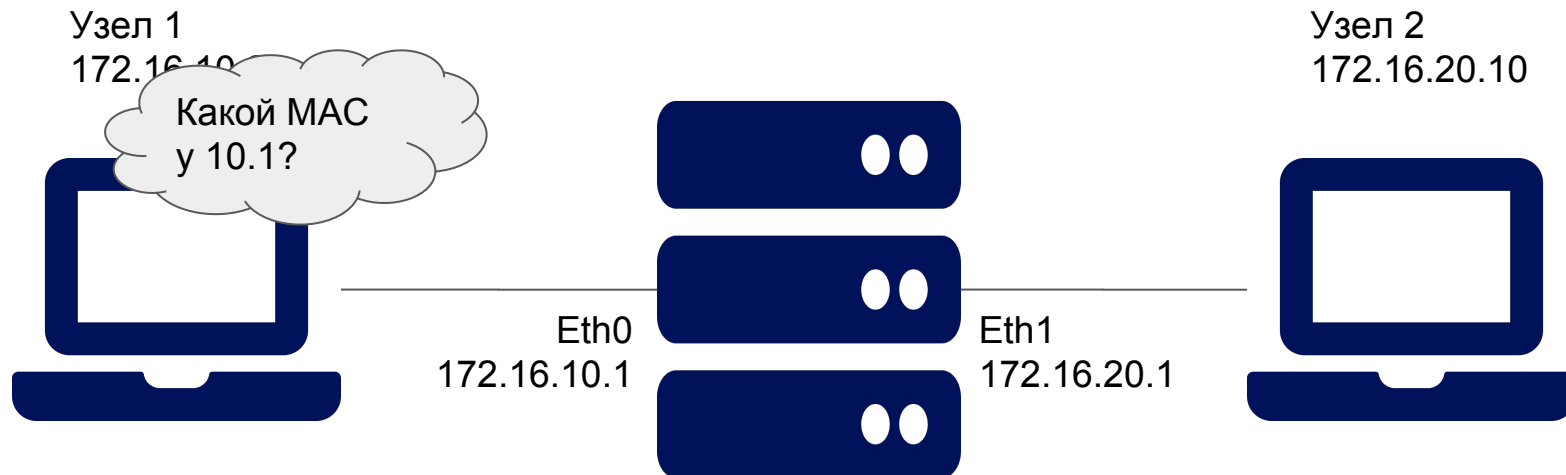
Eth1
172.16.20.1

Узел 2
172.16.20.10



Пример маршрутизации пакета

Для отправки на 172.16.10.1 по Ethernet
нужно знать его MAC адрес
Отправляется запрос в ARP-таблицу

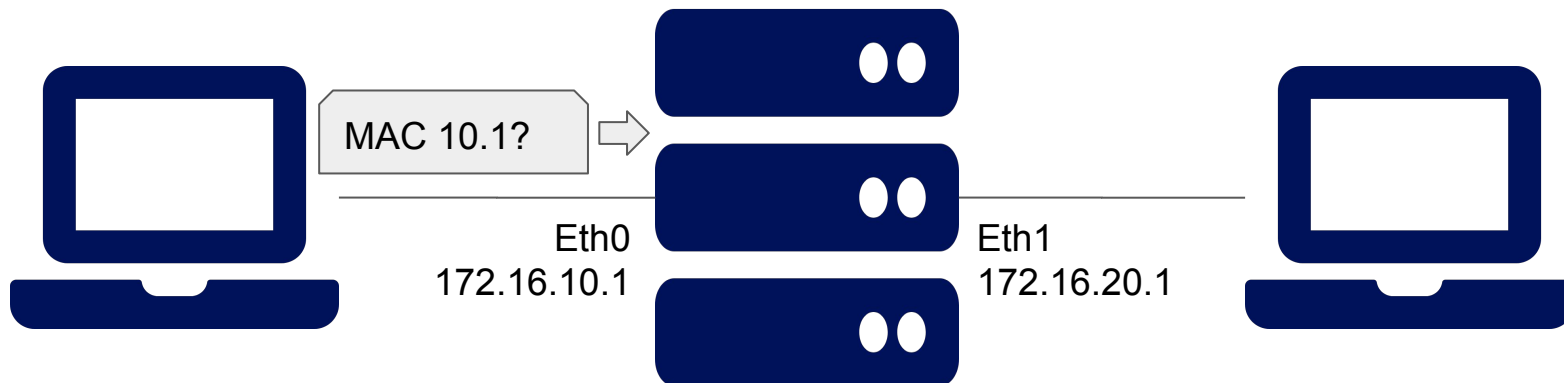


Пример маршрутизации пакета

Если в таблице нет этой записи, то
отправляется широковещательный
запрос ARP

Узел 1
172.16.10.2

Узел 2
172.16.20.10



Пример маршрутизации пакета

Маршрутизатор сообщает свой
MAC адрес интерфейса Eth0

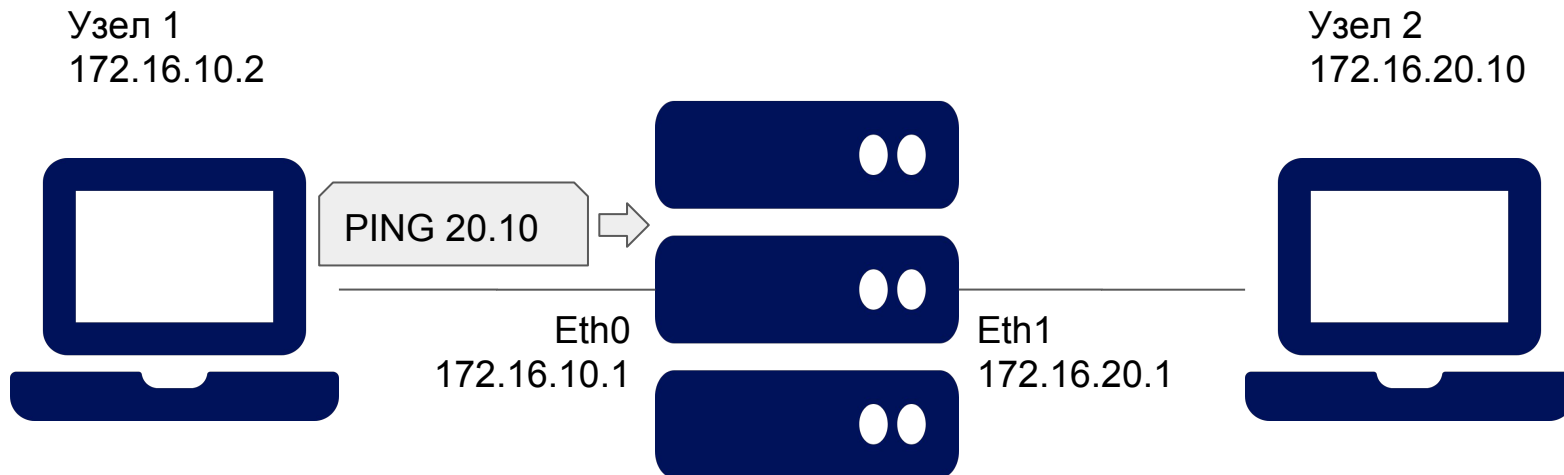
Узел 1
172.16.10.2

Узел 2
172.16.20.10



Пример маршрутизации пакета

10.2 знает MAC маршрутизатора.
Инкапсулирует ICMP в IP, а IP в Eth



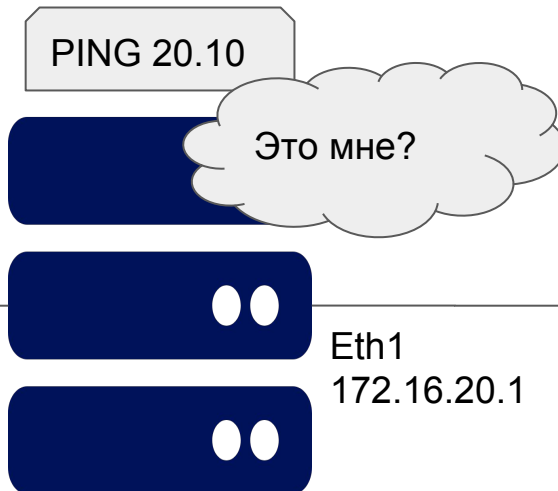
Пример маршрутизации пакета

Так как у пакета указан аппаратный адрес маршрутизатора, то он его принимает. Пакет передается на уровень IP

Узел 1
172.16.10.2



Eth0
172.16.10.1



Узел 2
172.16.20.10



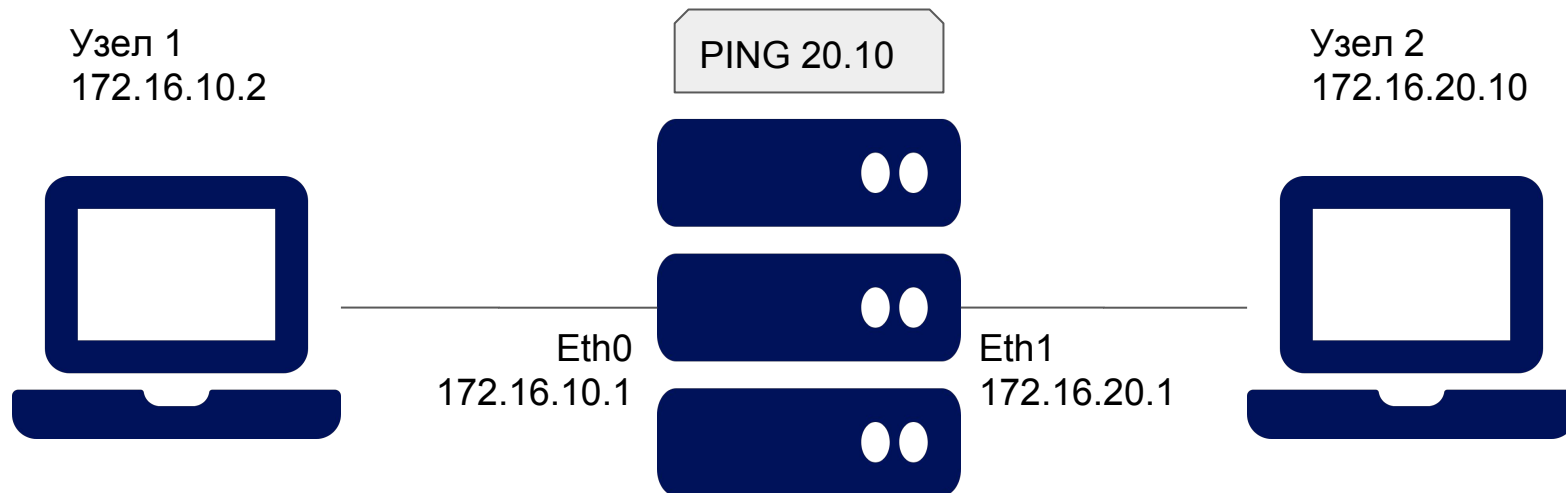
Пример маршрутизации пакета

Происходит проверка IP адреса. Он не соответствует адресу самого маршрутизатора. Следовательно, подлежит пересылке дальше.



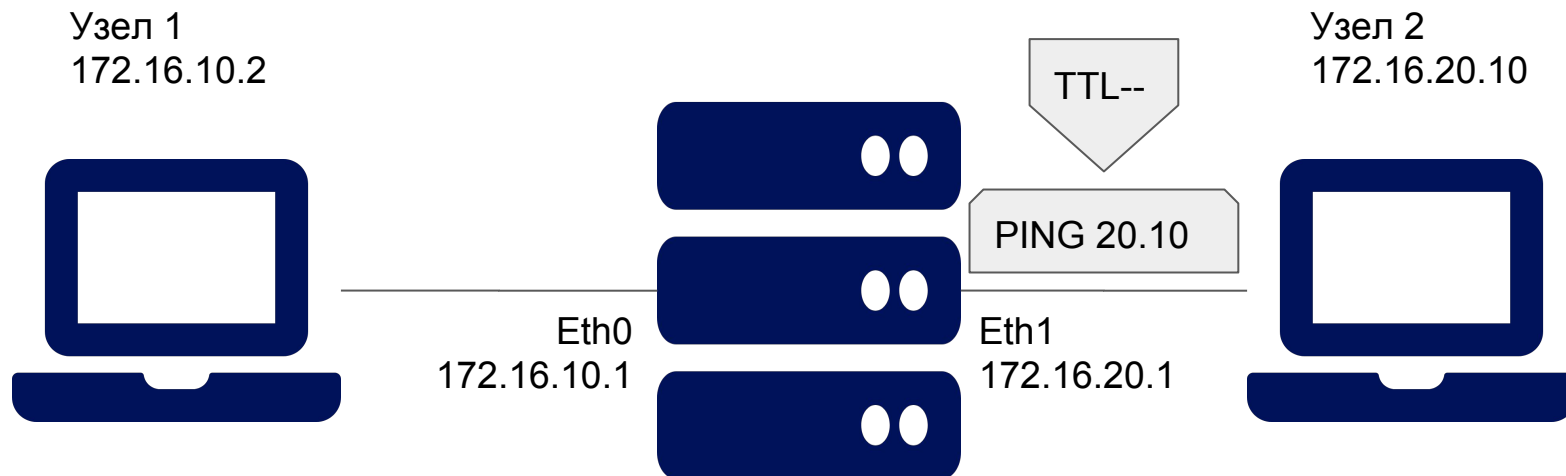
Пример маршрутизации пакета

Маршрутизатор анализирует поле IP адреса и обнаруживает, что пакет предназначен узлу подключенному к интерфейсу Eth1



Пример маршрутизации пакета

Маршрутизатор декрементирует поле TTL. Устанавливает аппаратный адрес получателя соответствующий узлу 2 и отправляет через интерфейс Eth1



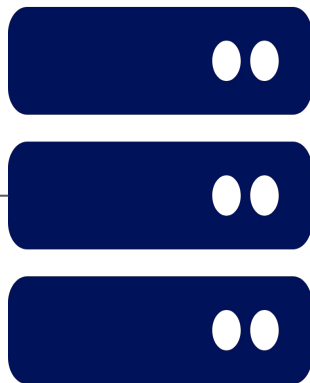
Пример маршрутизации пакета

Узел 2 принимает пакет. Так как аппаратный и IP адрес соответствуют его собственным принимает и обрабатывает запрос. Ответ отправляется аналогичным образом.

Узел 1
172.16.10.2



Eth0
172.16.10.1



Eth1
172.16.20.1

Узел 2
172.16.20.10



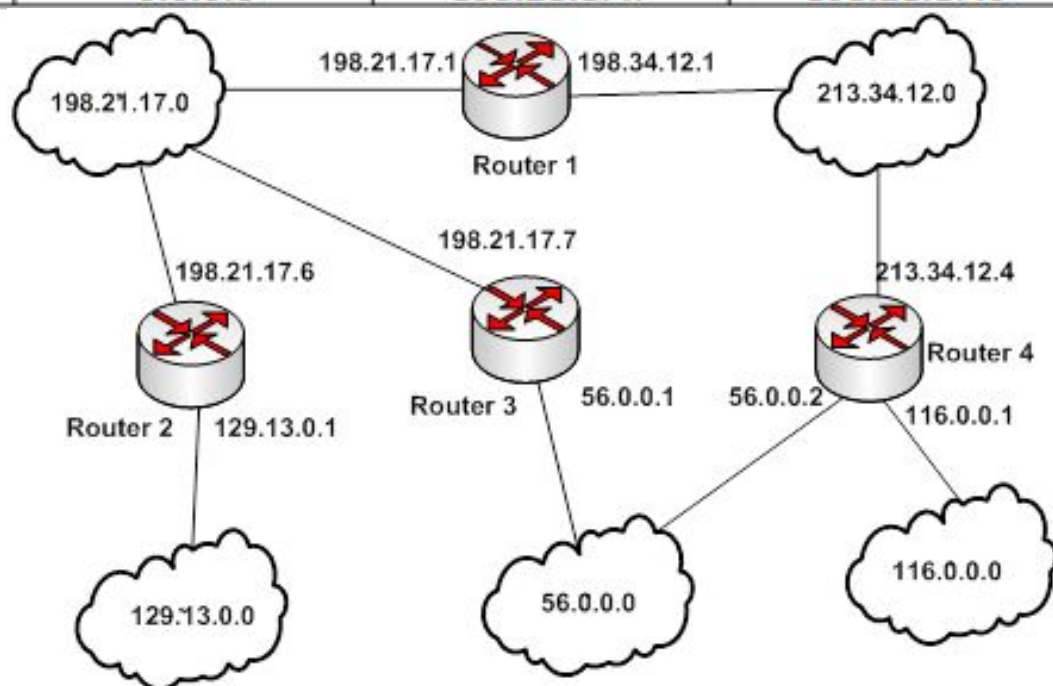
Таблицы маршрутизации

Таблица маршрутизации - это таблица соответствия сетей назначения и доступных сетевых интерфейсов.

Поля таблицы:

- Адрес сети\узла назначения
- Маска сети\узла
- Адрес шлюза, через который необходимо пересылать пакеты
- Метрика - “стоимость” пересылки

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
129.13.0.0	255.255.0.0	-	129.13.0.1	подключен
198.21.17.0	255.255.255.0	-	198.21.17.6	подключен
213.34.12.0	255.255.255.0	198.21.17.1	198.21.17.6	1
56.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	1
116.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	2
116.0.0.0	255.0.0.0	198.21.17.1	198.21.17.6	2
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.6	-



Закольцованные маршруты

При некорректно настроенной таблице маршрутизации, пакеты могут попадать безвыходное положение

Решение:

- При каждой пересылке через маршрутизатор значение TTL ip-датаграммы уменьшается на 1
- При достижении 0 такой пакет уничтожается

Transport layer - транспортный уровень

- Обеспечивает контроль передачи и проверку получения данных
 - Обнаружение дублирования и потери пакетов
-
- TCP
 - UDP
 - SPX

UDP - быстро и ненадежно

Особенности:

- Не устанавливается подключение между узлами
- Нет контроля доставки датаграмм на уровне протокола
- Низкий оверхед - заголовок всего 4-8 байт

Область применения:

- Стриминг аудио\видео данных и звонков
- Виртуальные сети
- Передача данных между приложениями с собственными алгоритмами контроля доставки

Порт подключения (UDP/TCP и др.)

Порт - это число в диапазоне от 1 до 65535 использующееся для указания программы которой предназначена посылка.

Номера портов регламентируются IANA. Весь диапазон разбит на 3 группы:

- 1-1024 порты - используют зарегистрированные системные службы
- 1024 - 49152 - используют пользовательские зарегистрированные службы
- 49152 - 65537 - используются для временных обменов данными

Широко используемые порты

- 20/21 - FTP - служба доступа к файлам
- 22 - SSH - служба удаленного доступа для управления компьютером
- 80 - Небезопасное HTTP подключение
- 443 - Безопасное HTTPS подключение
- 666 - сервер игры DOOM

Структура UDP пакета

Биты	0-15	16-31
0-31	Порт отправителя	Порт получателя
32-63	Длина пакета	Чексумма
64-..	Данные	

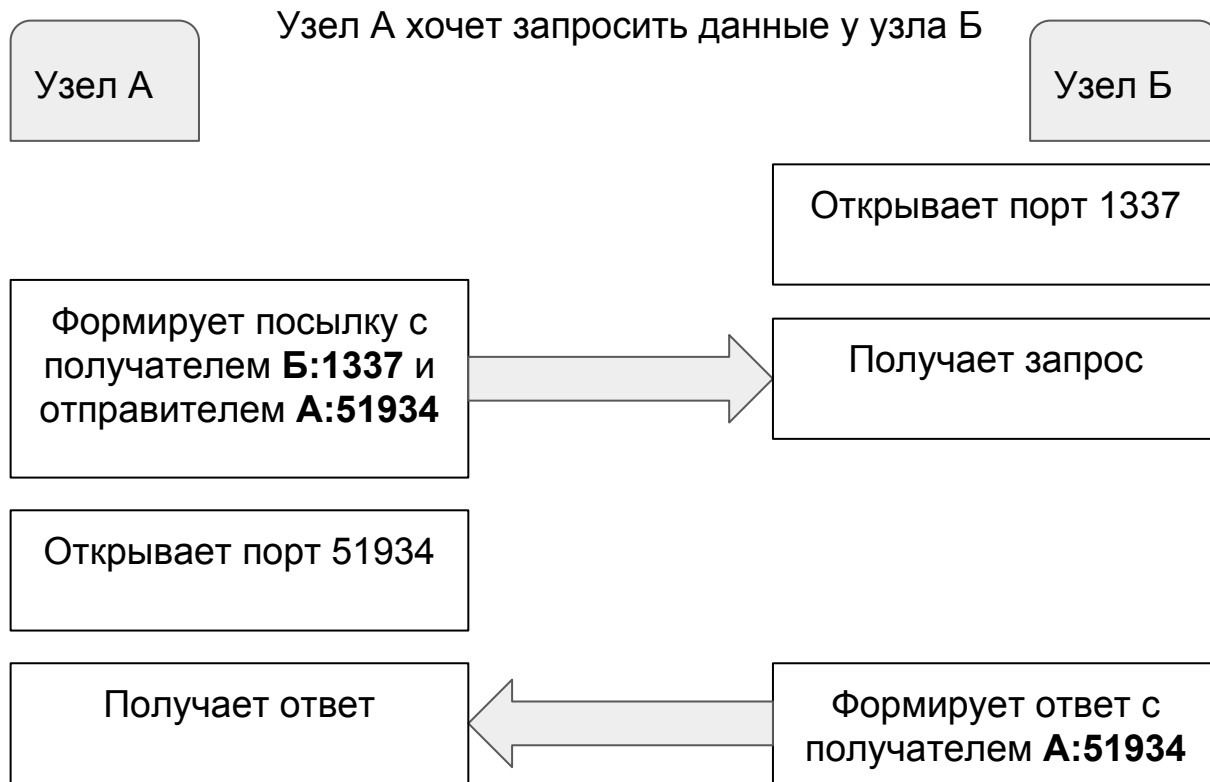
- Порт отправителя и чексумма могут не указываться
- Максимальная длина данных - 65507 байт. Реально - 508

Передача данных используя UDP

Узел А хочет передать данные
на узел Б



Запрос данных используя UDP



TCP - медленно, но верно

Особенности:

- Гарантирует доставку данных. Каждый переданный пакет подтверждается получателем
- Гарантирует доставку данных в правильном порядке. Каждый пакет пронумерован
- Использует двустороннее подключение

Область применения:

- Передача файлов и других данных, когда необходим контроль целостности

Структура TCP пакета

Биты	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт источника, Source Port			Порт назначения, Destination Port
32	Порядковый номер, Sequence Number (SN)			
64	Номер подтверждения, Acknowledgment Number (ACK SN)			
96	Длина заголовка	Резерв	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции			
160/192 +	Данные			

Флаги TCP пакета

- SYN — синхронизация номеров последовательности
- FIN — указывает на завершение соединения
- RST — оборвать соединения
- ACK — поле «Номер подтверждения» задействовано
- URG — поле «Указатель важности» задействовано
- PSH — протолкнуть данные в приложение пользователя

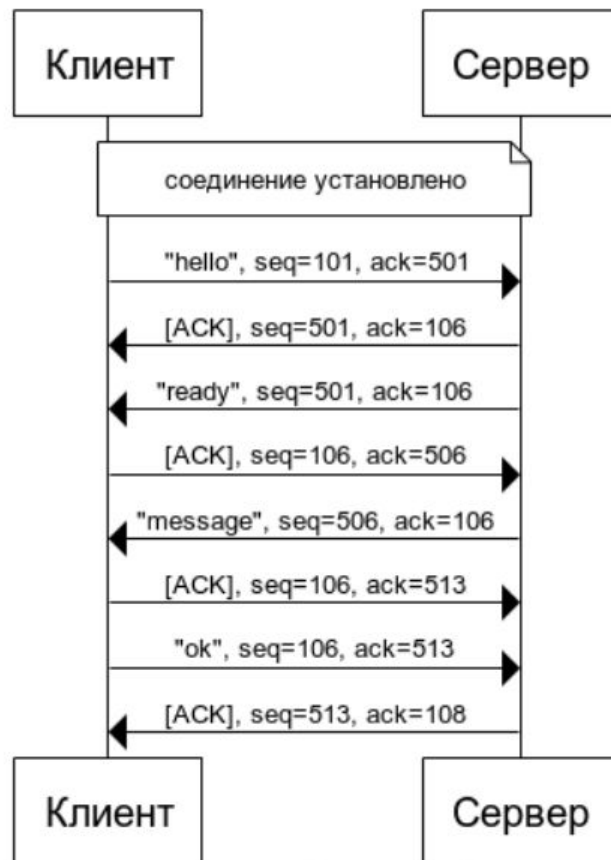
Механизм работы TCP

- Установка соединения
- Передача данных
- Завершение соединения

Установка соединения TCP



Передача данных



Завершение соединения



Session, Presentation, Application

- Определяют вид и представление информации на пользовательском уровне
- HTTP/WWW
- NFS/SMB/Bonjour
- SMTP/IMAP
- XMMP