Информационные сети

TCP\IP

План лекции:

- История TCP/IP
- Архитектура стека
- Поток данных по стеку
- Адресация на разных уровнях
- Примеры протоколов разных уровней
- IP адреса, классы, маски, специальные адреса, локальные диапазоны.
- Заголовок IP пакета. Фрагментация.

Стек TCP/IP

Стек TCP/IP – это набор иерархически упорядоченных сетевых протоколов.

Название стек получил по двум важнейшим протоколам:

- **TCP** (Transmission Control Protocol);
- **IP** (Internet Protocol).

Стек протоколов TCP/IP обладает двумя важными свойствами:

- платформонезависимость;
- открытость.

История создания

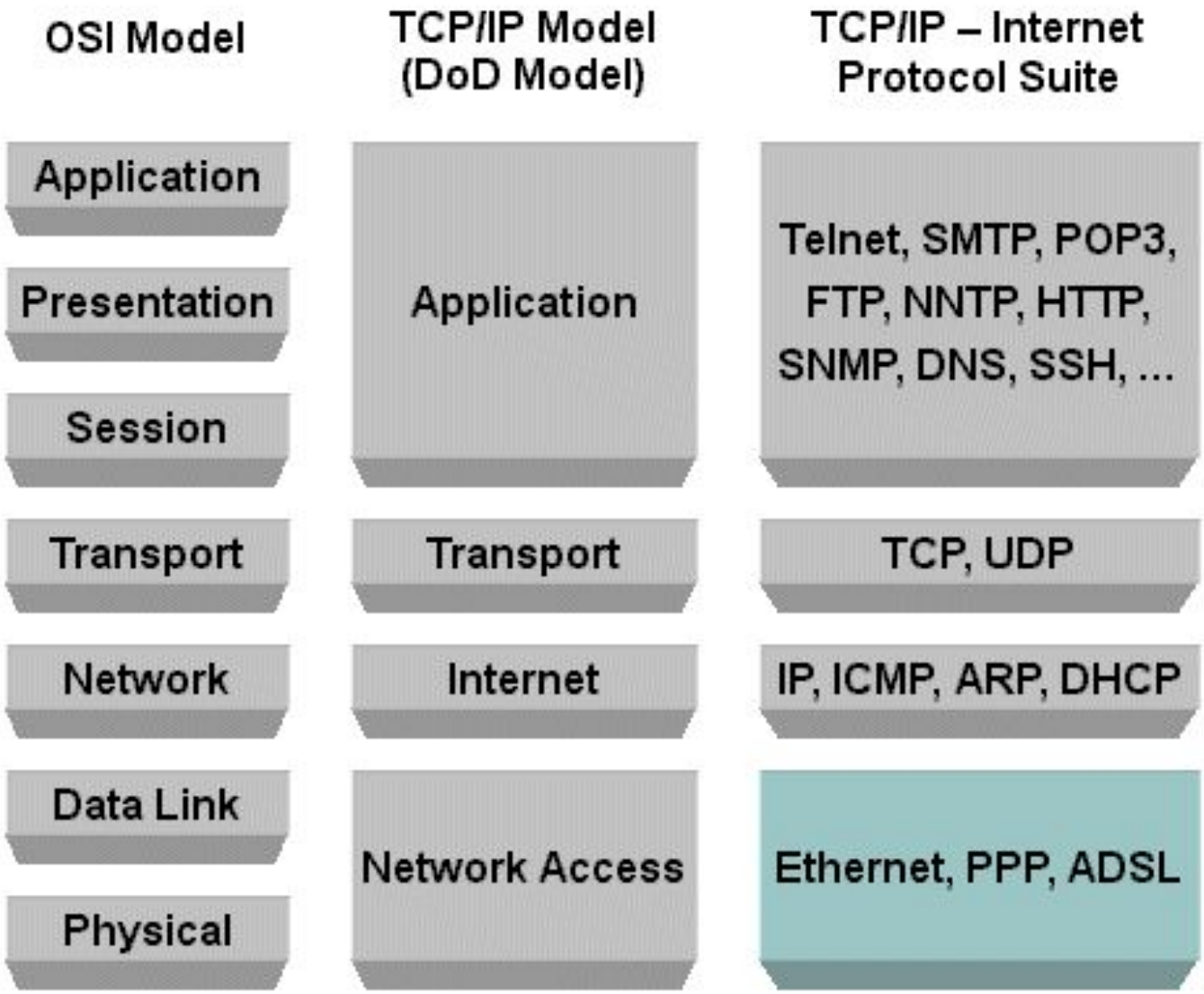
В **1967** году Агентство по перспективным исследовательским проектам министерства обороны США (**ARPA** – Advanced Research Projects Agency) инициировало разработку компьютерной сети, связывающей ряд университетов и научно-исследовательских центров, выполнявших заказы Агентства (**ARPANET** – в 1972 году соединяла 30 узлов).

В рамках проекта ARPANET были разработаны и в **1980–1981** годах опубликованы основные протоколы стека TCP/IP – **IP, TCP и UDP**. (Модель **OSI** утверждена в **1984**).

Важным фактором распространения TCP/IP стала его реализация в операционной системе **UNIX 4.2 BSD** (1983) университетом Беркли.

К концу 80-х годов ARPANET стала называться Интернет (**Interconnected networks** – связанные сети) и объединяла университеты и научные центры США, Канады и Европы.
Подразделение Internet Engineering Task Force (IETF) вносит основной вклад в совершенствование стандартов стека, публикуемых в форме спецификаций RFC.

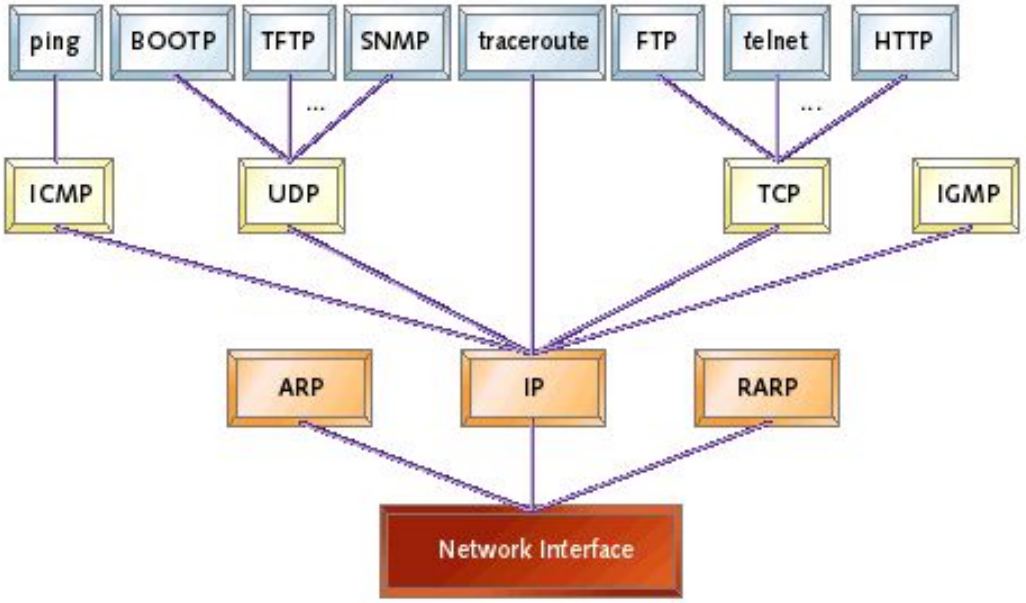
Архитектура стека (модель DARPA или DoD)



Примечание

Следует заметить, что **нижний уровень** модели DARPA (уровень сетевых интерфейсов) **не выполняет** функции канального и физического уровней, а лишь **обеспечивает связь** (интерфейс) верхних уровней DARPA с технологиями сетей, входящих в составную сеть (например, Ethernet, FDDI, ATM).

Поток данных по стеку



Адресация на разных уровнях

Соотнесите сетевые идентификаторы с уровнями стека TCP/IP:

1. MAC
2. IP
3. Port
4. Socket

Протоколы стека TCP/IP

Уровень приложений	**FTP SMTP POP3 IMAP4 HTTP RDP SSH Telnet DNS LDAP**		
Транспортный уровень	**TCP**	**UDP**	**XTP**
Межсетевой уровень	**ICMP ARP RARP**	**IP**	**DHCP BOOTP ESP AH RIP OSPF BGP EGP**
Уровень сетевого интерфейса	**PPTP L2F SLIP**		Интерфейсы к Ethernet, ATM, FDDI, WiFi И т.д.

Описание некоторых протоколов

- FTP (англ. File Transfer Protocol — протокол передачи файлов) – работает по протоколу TCP, порты 20 и 21. Предназначен для передачи файлов межу сервером и клиентом. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- SMTP (англ. Simple Mail Transfer Protocol — простой протокол передачи почты) – работает по 25 порту TCP, предназначен для передачи сообщений электронной почты между клиентским программным обеспечением и сервером, а также между серверами. Не содержит стандартных средств авторизации отправителя (кроме расширений ESMTP для авторизации клиента).
- POP3 (англ. Post Office Protocol Version 3 - протокол почтового отделения, версия 3) – работает по 110 порту TCP. Предназначен для получения клиентом почтовых сообщений с сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- HTTP (сокр. от англ. HyperText Transfer Protocol — протокол передачи гипертекста). Работает по портам 80, 8080 TCP. Предназначен для передачи текстовых и мультимедийных данных от сервера к клиенту по запросу последнего. В настоящее время используется как транспорт для других протоколов прикладного уровня.
- SSH (англ. Secure SHell — «безопасная оболочка») — сетевой протокол сеансового уровня
- Telnet (англ. TErminaL NETwork — протокол терминального сетевого доступа). Работает по 21 порту TCP. Предназначен для организации полнодуплексного сетевого терминала между клиентом и сервером. Команды выполняются на стороне сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- DNS (англ. Domain Name System — система доменных имён). Работает по портам 53 UDP для взаимодействия клиента и сервера и 53 TCP для AFXR запросов, поддерживающих обмен между серверами. DNS – протокол поддерживающий работу одноименной распределённой системы, осуществляющей отображение множества доменных имен и множества IP адресов хостов.
- TCP (анг. Transmission Control Protocol - протокол управления передачей). Протокол транспортного уровня, обеспечивающий установку двунаправленного соединения между процессами, идентифицирующимися по сокету (комбинации IP адреса и порта), передачу потока сегментов внутри соединения с подтверждением приема, управление и завершение соединения. Сообщение TCP содержит в заголовке адреса сегментов в направленном потоке и контрольную сумму при расчете которой используется поле данных и заголовок. Для оптимизации передачи и предотвращения перегрузок сети используется механизм переменного окна, позволяющий вести передачу без получения подтверждения приема каждого сообщения. В качестве адресной информации использует порт.
- UDP (англ. User Datagram Protocol — протокол пользовательских дейтаграмм). Протокол транспортного уровня, обеспечивающий передачу сообщений между процессами, идентифицирующимися по сокету (комбинации IP адреса и порта). Сеанс не устанавливается, подтверждения приема не осуществляется. В качестве адресной информации использует порт.

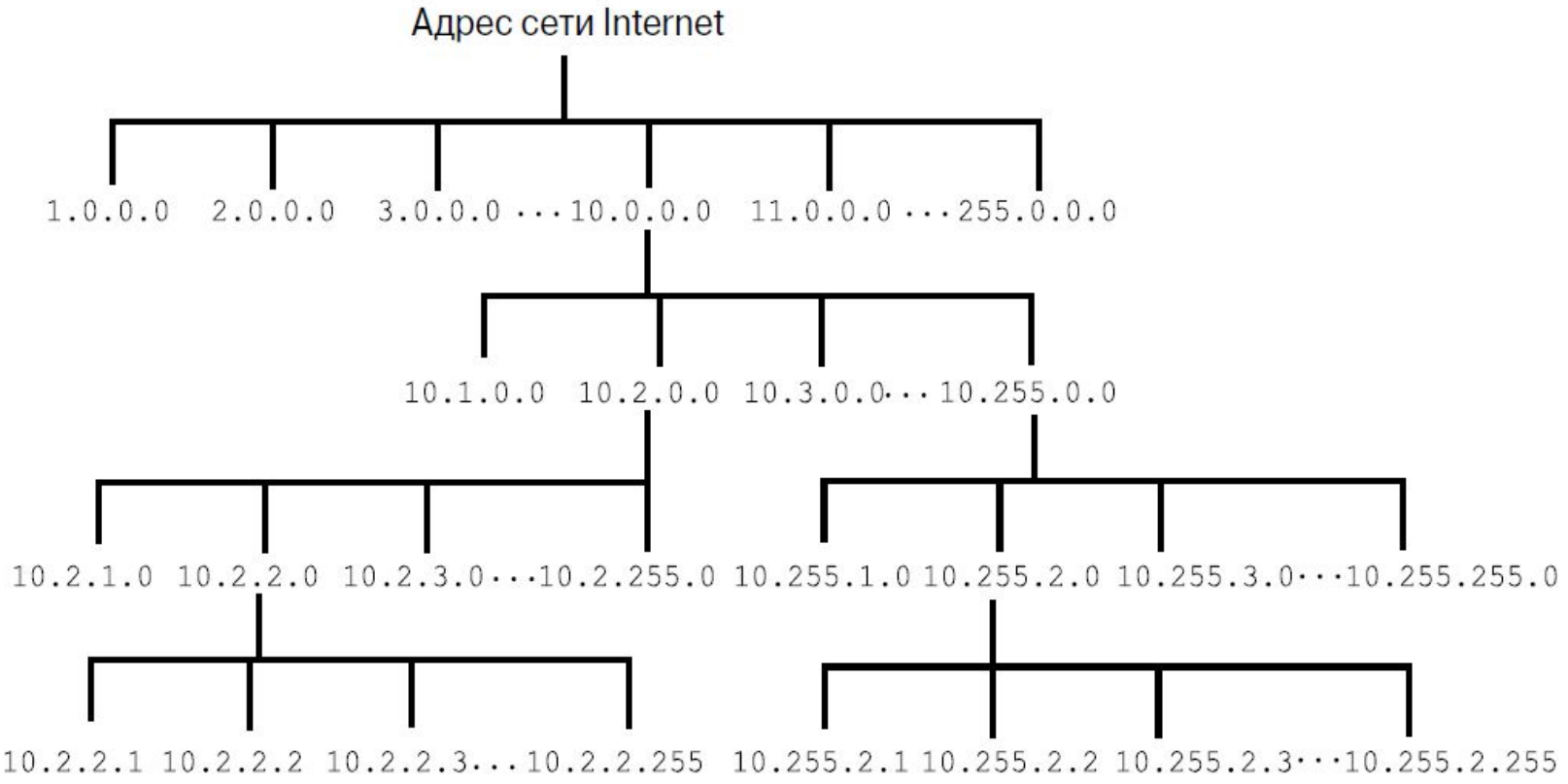
IP - адресация

IP-адрес – это уникальный числовой адрес, однозначно идентифицирующий узел, группу узлов или сеть.

IPv4-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел «**октетов**», разделенных точками – W.X.Y.Z

Каждый октет может принимать значения в диапазоне от 0 до 255.

Иерархическая адресация



Иерархические IP-адреса

Классы IP-адресов

Классы IP-адресов					
Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в десятичном и двоичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей (2^7-2) 16 777 214 узлов для каждой сети (2^24-2)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей (2^14-2) 65 534 узла для каждой сети (2^16-2)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей (2^21-2) 254 узла для каждой сети (2^8-2)
D	224 - 239	11100000 - 11101111	В качестве узла не для коммерческого использования		
E	240 - 255	11110000 - 11111111	В качестве узла не для коммерческого использования		

Классовая и бесклассовая адресация

- **Классовая IP адресация** — это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. не возможно использование различных масок подсетей. В классовом методе адресации используется фиксированная маска подсети, поэтому класс сети всегда можно идентифицировать по первым битам.
- **Бесклассовая IP адресация (*Classless Inter-Domain Routing — CIDR)*** — это метод IP-адресации, который позволяет рационально управлять пространством IP адресов. В бесклассовом методе адресации используются маски подсети переменной длины (*variable length subnet mask — VLSM*).

Публичные и частные IP-адреса

В соответствии со стандартом RFC 1918 было зарезервировано несколько диапазонов адресов класса A, B и C.

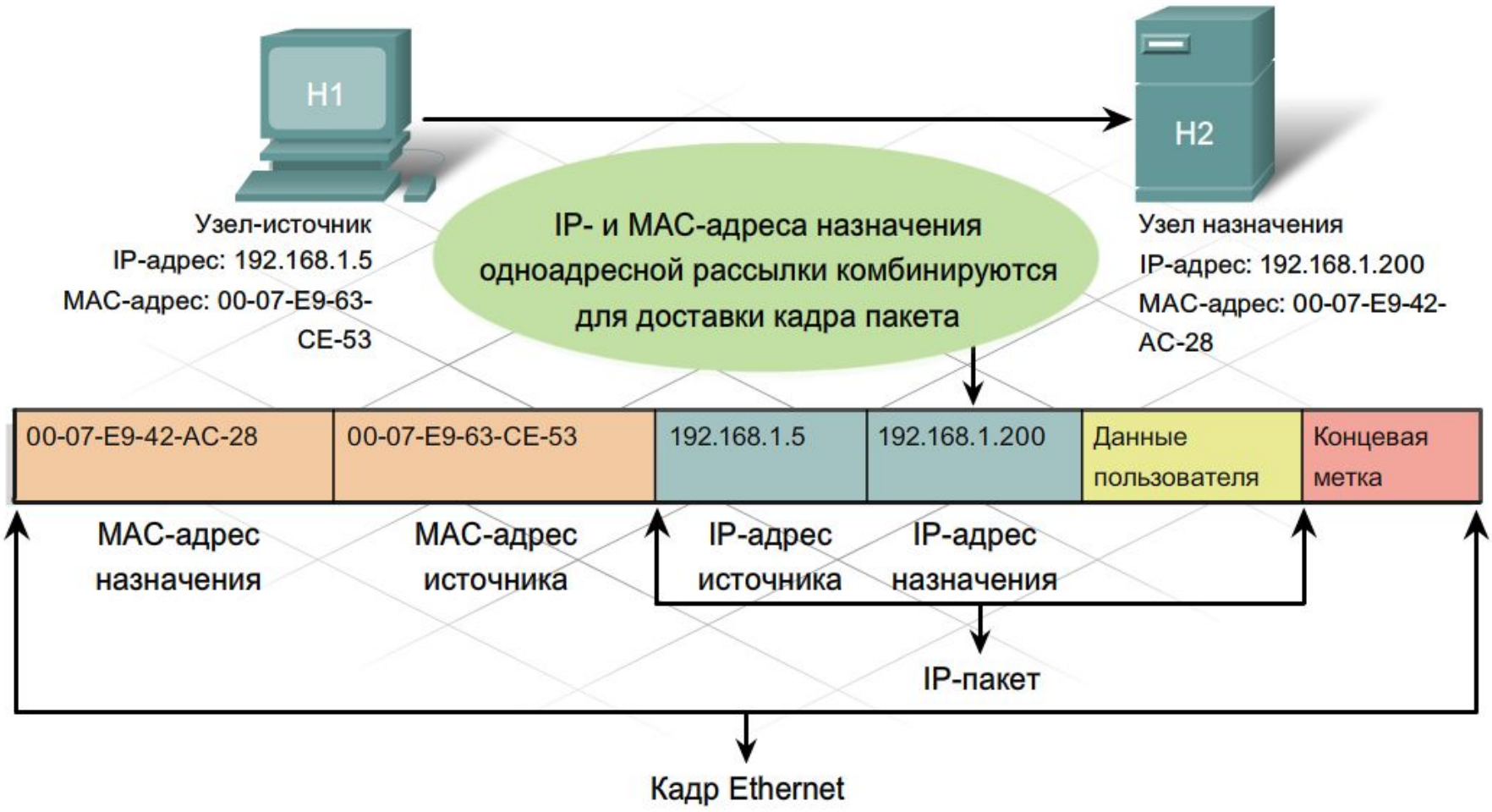
Класс адреса	Число зарезервированных сетевых адресов	Сетевые адреса
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Типы рассылок

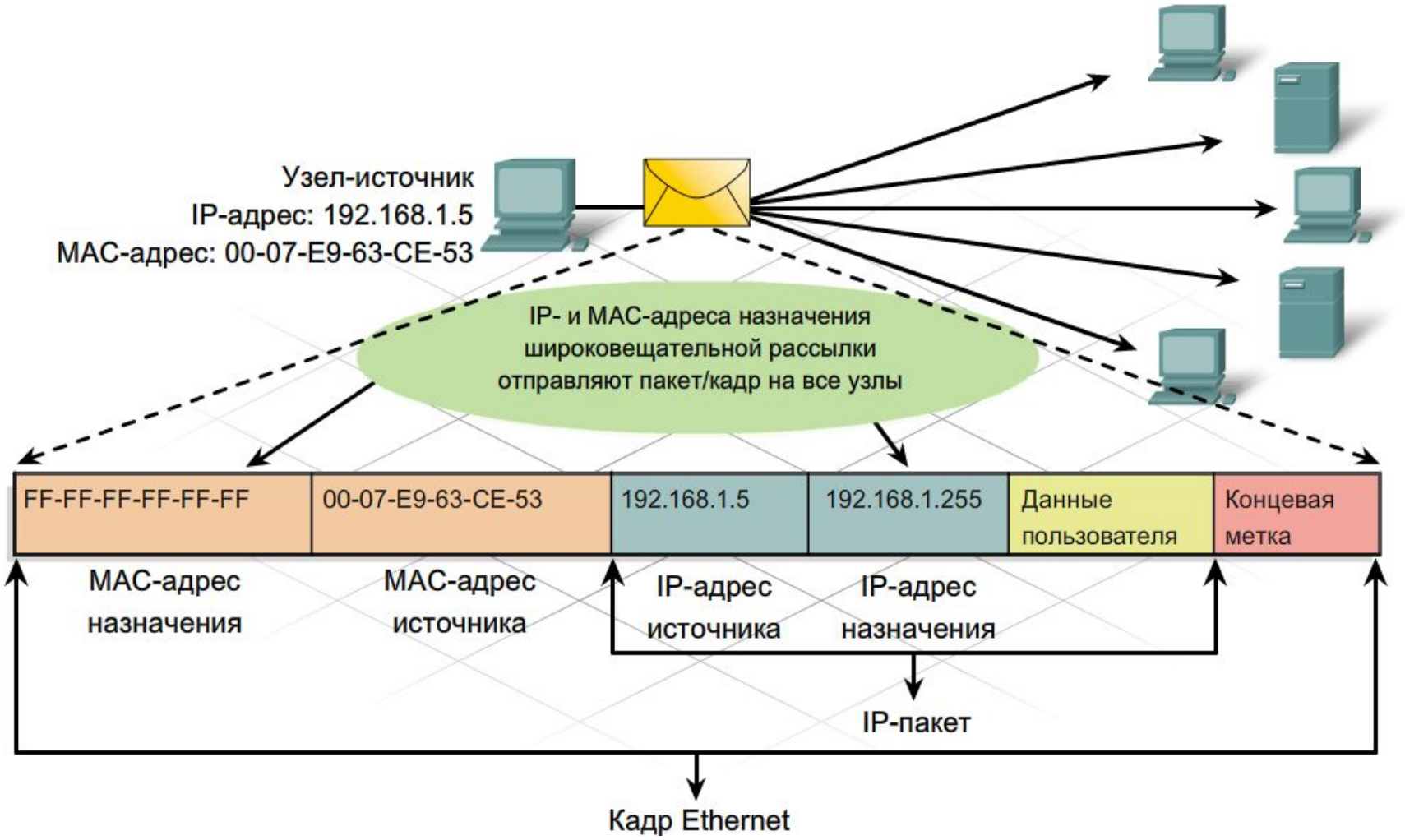
Помимо классов, IP-адреса делятся на категории, предназначенные для разных типов рассылок:

- «один к одному» (одноадресная рассылка);
- «один ко многим» (многоадресная рассылка);
- «один ко всем» (широковещательная рассылка).

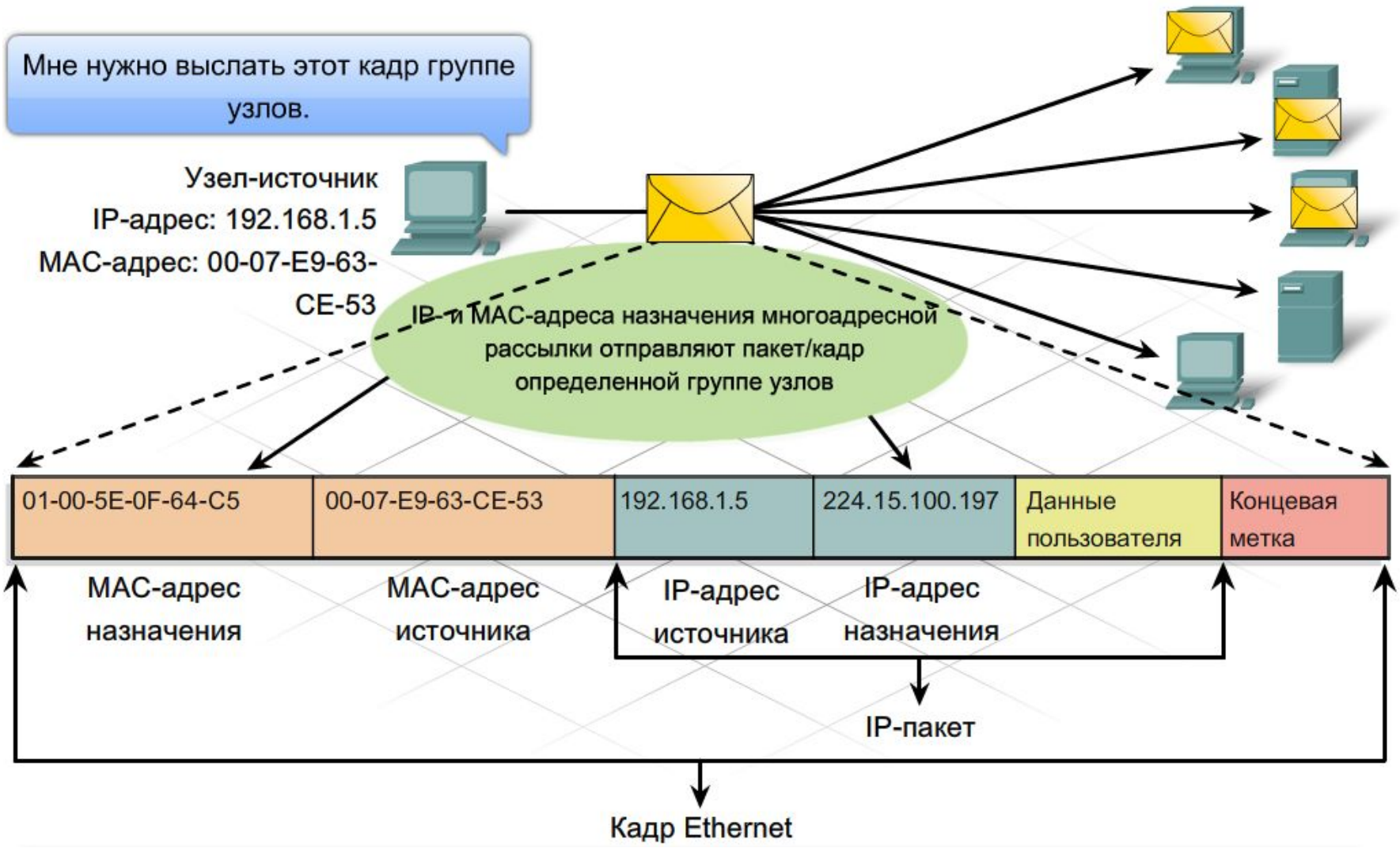
Одноадресная рассылка



Широковещательная рассылка



Многоадресная рассылка

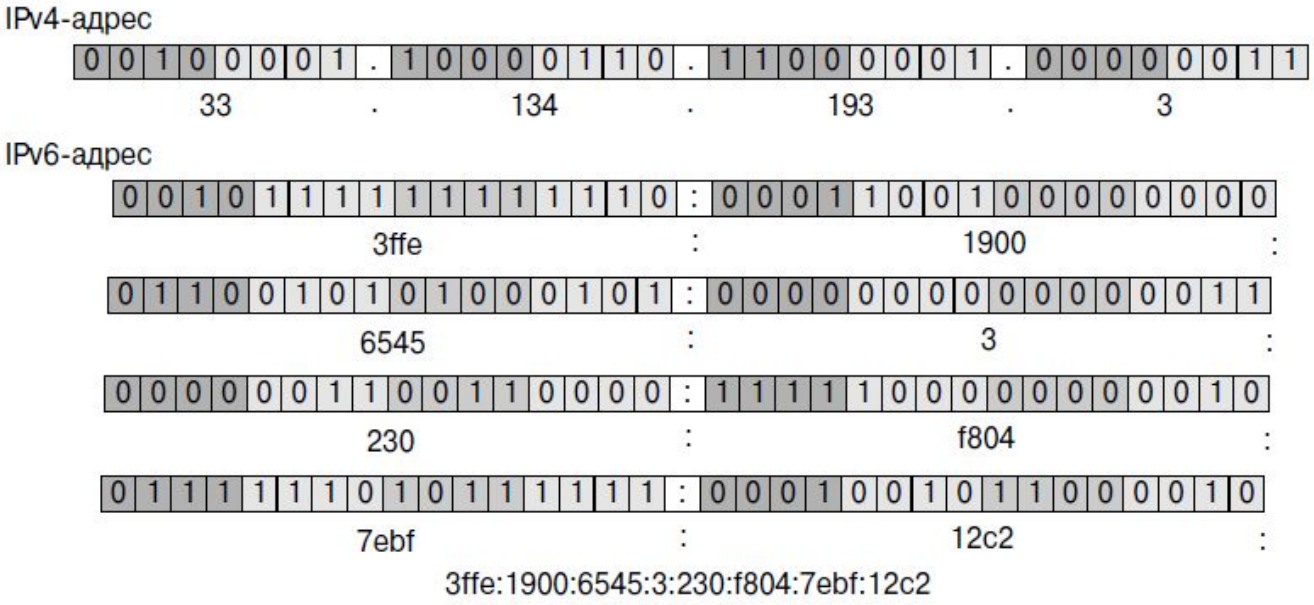


IPv4 vs IPv6

Internet-протокол версии 4 (IPv4) 4 октета
11010001.11011100.11001001.01110001
209.156.201.113
4,294,467,295 IP-адресов

Internet-протокол версии 6 (IPv6) 16 октетов
11010001.11011100.11001001.01110001.11010001.11011100. 110011001.01110001.11010001.11011100.11001001. 01110001.11010001.11011100.11001001.01110001
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73
3.4 x 10^{38} IP-адресов

Сравнение стандартов IPv4 и IPv6



Форматы адресов IPv4 и IPv6

Заголовок IP-пакета

IP-фрагментация и реассемблирование

Максимальная длина датаграммы IP - 64 КБ.
Большинство каналов передачи данных устанавливают максимальный предел длины пакета (**MTU**).

Значение MTU зависит от типа канала передачи данных. Дизайн IP протокола приспосабливается к различным MTU, разрешая маршрутизаторам фрагментировать IP датаграммы.

За сборку (реассемблирование) фрагментов обратно в оригинальную IP датаграмму полного размера ответственна принимающая сторона.

IP-фрагментация это разбиение датаграммы на множество частей, которые могут быть повторно собраны позже.

Для IP-фрагментации и повторной сборки используются поля из IP заголовка:

- источник;
- адресат;
- идентификация;
- полная длина;
- смещение фрагмента;
- 2 флажка: "больше фрагментов" (MF) и "не фрагментировать" (DF).

Пример фрагментации

Original IP Datagram

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Первый фрагмент имеет смещение 0, длина этого фрагмента - 1500; она включает 20 байтов для измененного оригинального IP заголовка.
Второй фрагмент имеет смещение 185 (185 x 8 = 1480), которое означает, что порция данных этого фрагмента начинается с 1480 байта в оригинальной IP датаграмме. Длина этого фрагмента - 1500; она включает дополнительный IP заголовок, созданный для этого фрагмента.
Третий фрагмент имеет смещение 370 (370 x 8 = 2960), которое означает, что данные этого фрагмента начинаются с 2960 байта в оригинальной IP датаграмме. Длина этого фрагмента - 1500; она включает дополнительный заголовок IP, созданный для этого фрагмента.
Четвертый фрагмент имеет смещение 555 (555 x 8 = 4440), которое означает, что часть данных этого фрагмента начинается с 4440 байтов в оригинальной IP датаграмме. Длина этого фрагмента - 700 байтов.

Если добавить байты данных от последнего фрагмента (680 = 700 - 20), это даст 5120 байтов, что является порцией данных оригинальной IP датаграммы. Затем, добавляя 20 байтов для IP заголовка мы получим размер оригинальной IP датаграммы (4440 + 680 + 20 = 5140).