

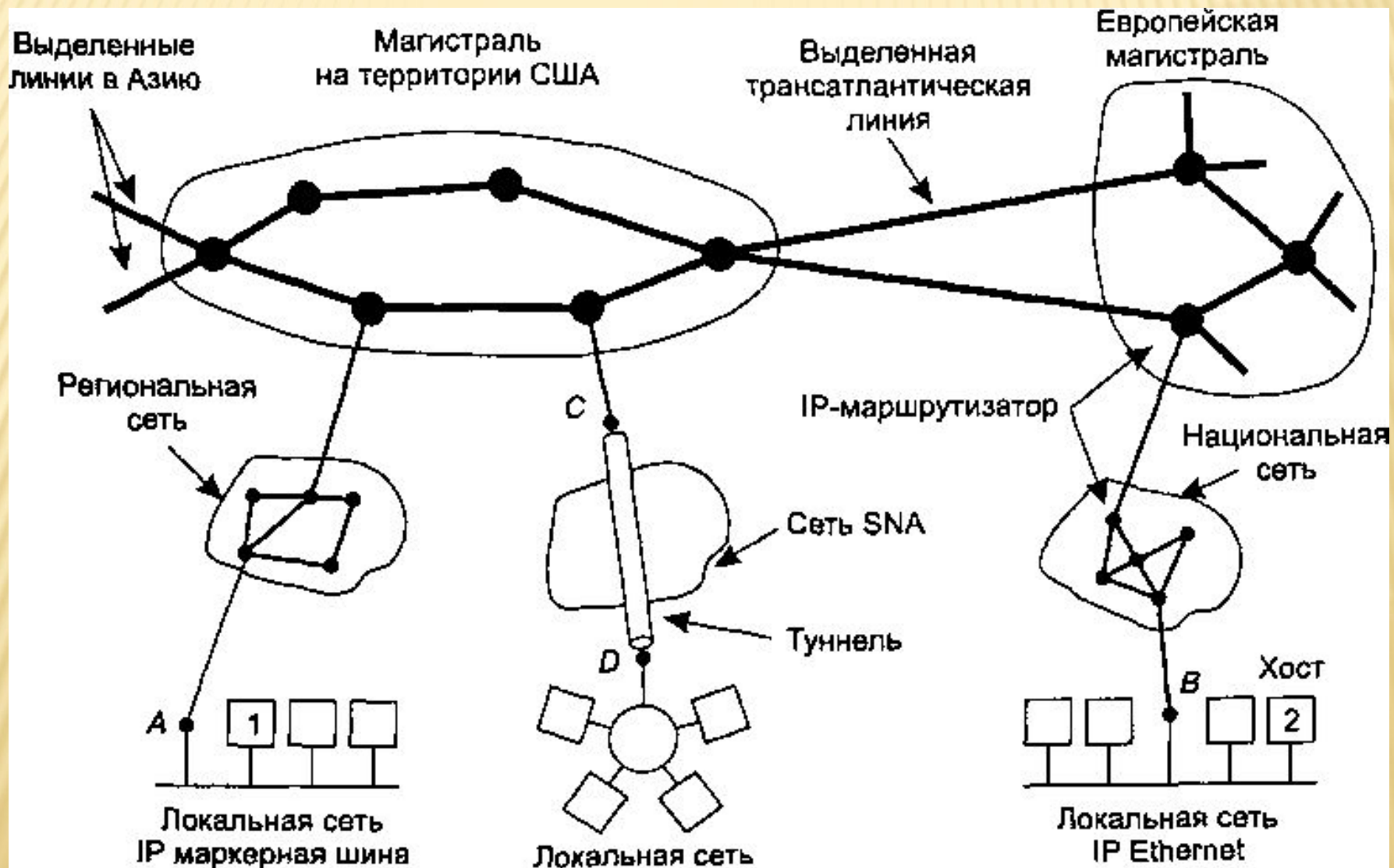
8. Сетевой уровень: IP протокол
Газизов Тимур Тальгатович,
к.т.н., доцент кафедры информатики ТГПУ

ИНФОРМАЦИОННЫЕ СЕТИ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

СЕТЕВОЙ УРОВЕНЬ В ИНТЕРНЕТЕ

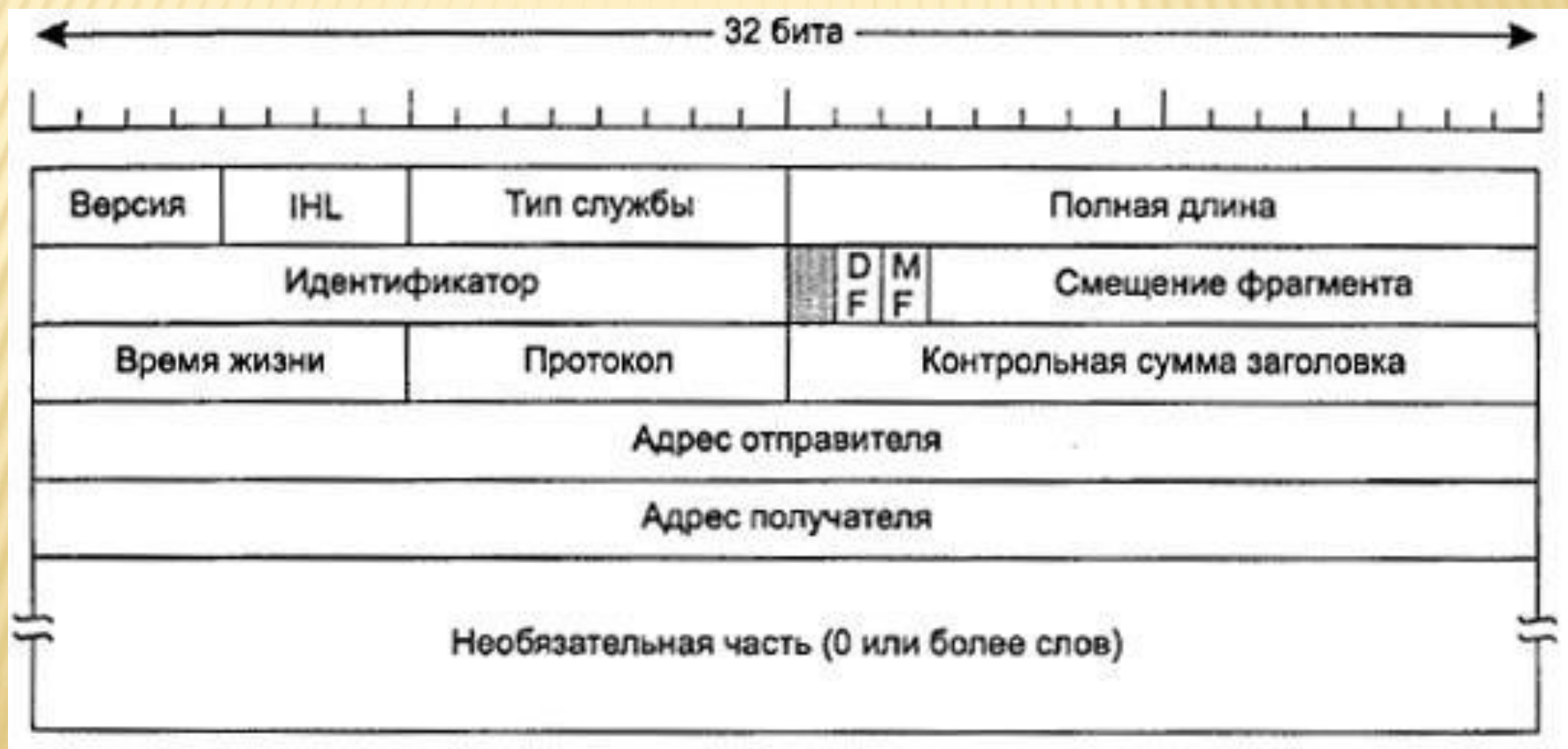
- На сетевом уровне Интернет можно рассматривать как набор подсетей или автономных систем, соединенных друг с другом. Структуры как таковой Интернет не имеет, но все же есть несколько магистралей. Они собраны из высокопроизводительных линий и быстрых маршрутизаторов. К магистралям присоединены региональные сети (сети среднего уровня), с которыми, в свою очередь, соединяются локальные сети многочисленных университетов, компаний и провайдеров

ИНТЕРНЕТ – НАБОР СЕТЕЙ



ПРОТОКОЛ IP

- IP-дейтаграмма состоит из заголовка и текстовой части. Заголовок содержит обязательную 20-байтную часть, а также необязательную часть переменной длины



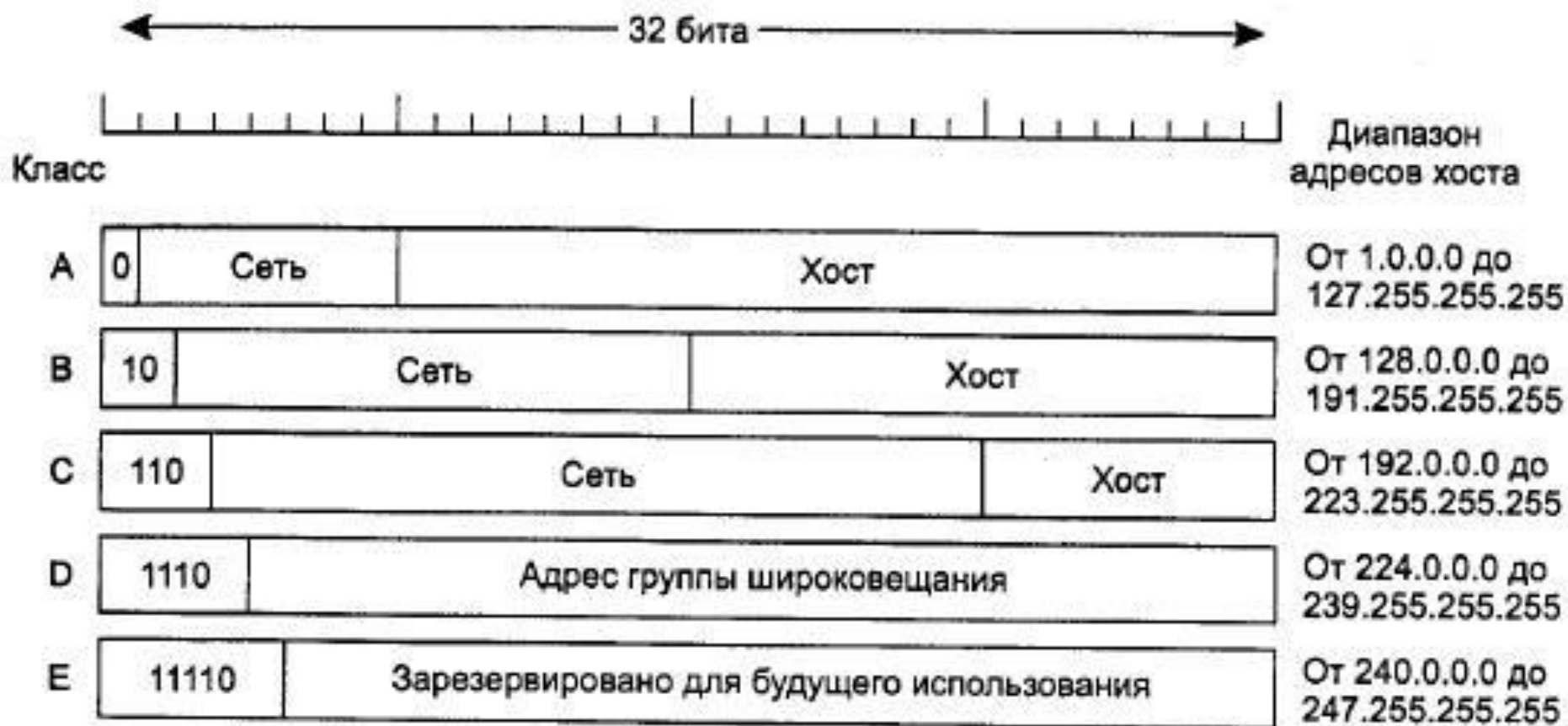
ПРОТОКОЛ IP

- Поле *Версия* содержит версию протокола, к которому принадлежит дейтаграмма
- Поле *Тип службы* – единственное поле, смысл которого с годами несколько изменился. Оно было (впрочем, и до сих пор) предназначено для различения классов обслуживания
- (На практике сегодняшние маршрутизаторы часто вообще игнорируют поле *Тип службы*.)
- Поле *Полная длина* содержит длину всей дейтаграммы, включая как заголовок, так и данные. Максимальная длина дейтаграммы 65 535 байт. В настоящий момент этот верхний предел достаточен, однако с появлением гигабитных сетей могут понадобиться дейтаграммы большего размера.
- Поля *Адрес отправителя* и *Адрес получателя* указывают номер сети и номер хоста.

IP-АДРЕСА

- У каждого хоста и маршрутизатора в Интернете есть IP-адрес, состоящий из номера сети и номера хоста. Эта комбинация уникальна: нет двух машин с одинаковыми IP-адресами.
- Все IP-адреса имеют длину 32 бита и используются в полях Адрес отправителя и Адрес получателя IP-пакетов.
- IP-адрес, на самом деле, не имеет отношения к хосту. Он имеет отношение к сетевому интерфейсу, поэтому хост, соединенный с двумя сетями, должен иметь два IP-адреса.

КЛАССЫ СЕТЕЙ



ПОЛНОКЛАССОВАЯ АДРЕСАЦИЯ

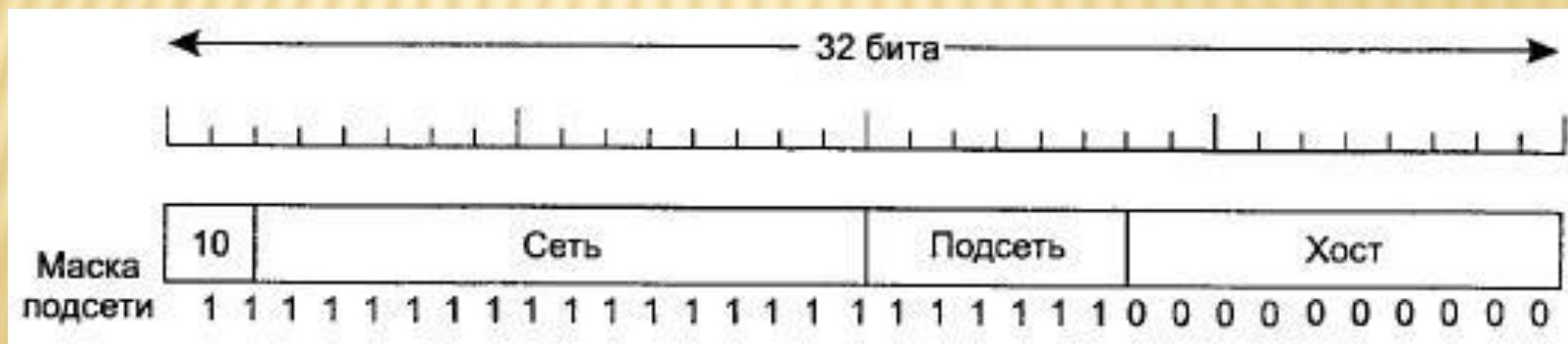
- Форматы классов А, В, С и D позволяют задавать адреса до 128 сетей с 16 млн хостов в каждой, 16 384 сетей с 64 тысячами хостов или 2 миллионов сетей (например, ЛВС) с 256 хостами (хотя некоторые из них могут быть специализированными)

ПОДСЕТИ

- Вместо одного адреса класса В с 14 битами для номера сети и 16 битами для номера хоста было предложено использовать несколько другой формат – формировать адрес подсети из нескольких битов. Например, если в университете существует 35 подразделений, то 6-битным номером можно кодировать подсети, а 10-битным – номера хостов. С помощью такой адресации можно организовать до 64 сетей Ethernet по 1022 хоста в каждой (адреса 0 и -1 не используются, как уже говорилось, поэтому не 1024 (2^{10}), а именно 1022 хоста). Такое разбиение может быть изменено, если окажется, что оно не очень подходит.

МАСКИ

- Маршрутизатор должен либо содержать таблицу из 64536 записей, либо использовать маску в паре с IP адресом, чтобы точно знать где номер сети, а где адрес
- маску подсети можно записать в виде 255.255.252.0. Альтернативная запись будет включать /22, показывая, что маска подсети занимает 22 бита.



CIDR – БЕСКЛАССОВАЯ МАРШРУТИЗАЦИЯ

- класс В слишком велик для большинства контор, которые устанавливают у себя сети. Исследования показали, что более чем в половине случаев сети класса В включают в себя менее 50 хостов
- С точки зрения маршрутизаторов, адресное пространство IP представляет собой двухуровневую иерархию, состоящую из номеров сетей и номеров хостов. Маршрутизаторы не обязаны знать номера вообще всех хостов, но им необходимо знать номера всех сетей
- проблема состоит в том, что сложность обработки этих таблиц растет быстрее, чем сами таблицы, то есть зависимость между ними не линейная

МАРАШРУТИЗАЦИЯ

- Допустим, имеется набор из миллионов адресов, начиная с 194.24.0.0. Допустим также, что Кембриджскому университету требуется 2048 адресов, и ему выделяются адреса от 194.24.0.0 до 194.24.7.255, а также маска 255.255.248.0. Затем Оксфордский университет запрашивает 4096 адресов. Так как блок из 4096 адресов должен располагаться на границе, кратной 4096, то ему не могут быть выделены адреса начиная с 194.24.8.0. Вместо этого он получает адреса от 194.24.16.0 до 194.24.31.255 вместе с маской 255.255.240.0. Затем Эдинбургский университет просит выделить ему 1024 адреса и получает адреса от 194.24.8.0 до 194.24.11.255 и маску 255.255.252.0.

ПРИМЕР

Университет	Первый адрес	Последний адрес	Количество	Форма записи
Кембридж	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Эдинбург	194.24.8.0	94.24.11.255	1024	194.24.8.0/22
(Свободно)	194.24.12.0	94.24.15.255	1024	194.24.12.0/22
Оксфорд	194.24.16.0	94.24.16.255	4096	194.24.16.0/20

ПРИМЕР

- После этого таблицы маршрутизаторов по всему миру получают три новые строки, содержащие базовый адрес и маску. В двоичном виде эти записи выглядят так:

Адрес	Маска
К: 11000010 00011000 00000000 00000000	11111111 11111111 11111000 00000000
Э: 11000010 00011000 00001000 00000000	11111111 11111111 11111100 00000000
О: 11000010 00011000 00010000 00000000	11111111 11111111 11110000 00000000
- Теперь посмотрим, что произойдет, когда пакет придет по адресу 194.24.17.4.
- В двоичном виде этот адрес представляет собой следующую 32-битную строку:
11000010 00011000 00010001 00000100
- Сначала на него накладывается (выполняется логическое И) маска Кембриджа, в результате чего получается
11000010 00011000 00010000 00000000
- Это значение не совпадает с базовым адресом Кембриджа, поэтому на оригинальный адрес накладывается маска Оксфорда, что дает в результате;
11000010 00011000 00010000 00000000
- Это значение совпадает с базовым адресом Оксфорда. Если далее по таблице совпадений нет, то пакет пересылается Оксфордскому маршрутизатору. Теперь посмотрим на эту тройку университетов с точки зрения маршрутизатора в Омахе, штат Небраска, у которого есть всего четыре выходных линии: на Миннеаполис, Нью-Йорк, Даллас и Денвер. Получив три новых записи, маршрутизатор понимает, что он может скомпоновать их вместе и получить одну агрегированную запись, состоящую из адреса 194.24.0.0/19 и подмаски:
11000010 00000000 00000000 00000000 11111111 11111111 11100000 00000000
- В соответствии с этой записью пакеты, предназначенные для любого из трех университетов, отправляются в Нью-Йорк. Объединив три записи, маршрутизатор в Омахе уменьшил размер своей таблицы на две строки.

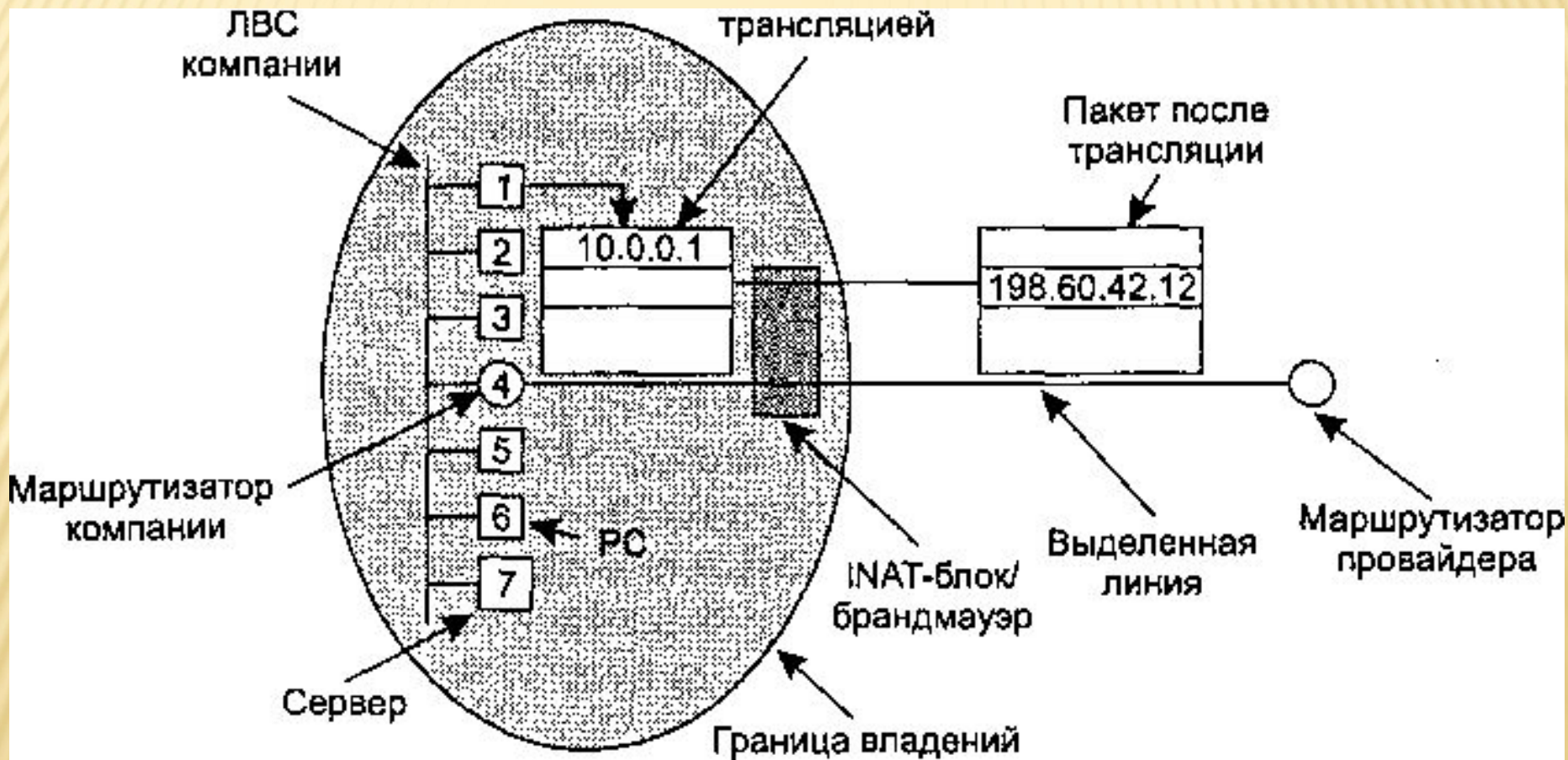
NAT – ТРАНСЛЯЦИЯ СЕТЕВОГО АДРЕСА

- IP-адреса являются дефицитным ресурсом. У провайдера может быть /16-адрес (бывший класс В), дающий возможность подключить 65 534 хоста. Если клиентов становится больше, начинают возникать проблемы. Хостам, подключающимся к Интернету время от времени по обычной телефонной линии, можно выделять IP-адреса динамически, только на время соединения. Тогда один /16-адрес будет обслуживать до 65 534 *активных* пользователей, и этого, возможно, будет достаточно для провайдера, у которого несколько сотен тысяч клиентов.

ТРАНСЛЯЦИИ СЕТЕВОГО АДРЕСА

- присвоении каждому клиенту (организации) одного IP-адреса (или, по крайней мере, небольшого числа адресов) для интернет-траффика. Внутри организации каждый компьютер получает уникальный IP-адрес, используемый для маршрутизации внутреннего траффика. Однако как только пакет покидает пределы здания фирмы и направляется к провайдеру, выполняется трансляция адреса.

РАСПОЛОЖЕНИЕ И РАБОТА NAT БЛОКА



NAT ПРИНЦИП РАБОТЫ

- С помощью поля *Порт источника* мы можем решить проблему отображения адресов. Когда исходящий пакет приходит в NAT-блок, адрес источника вида 10.x.y.z заменяется настоящим IP-адресом. Кроме того, поле *Порт источника* TCP заменяется индексом таблицы перевода NAT-блока, содержащей 65 536 записей. Каждая запись содержит исходный IP-адрес и номер исходного порта. Наконец, пересчитываются и вставляются в пакет контрольные суммы заголовков TCP и IP. Необходимо заменять поле *Порт источника*, потому что машины с местными адресами 10.0.0.1 и 10.0.0.2 могут случайно пожелать воспользоваться одним и тем же портом (5000-м, например). Так что для однозначной идентификации процесса отправителя одного поля *Порт источника* оказывается недостаточно.
- Когда пакет прибывает на NAT-блок со стороны провайдера, извлекается значение поля *Порт источника* заголовка TCP. Оно используется в качестве индекса таблицы отображения NAT-блока. По найденной в этой таблице записи определяются внутренний IP-адрес и настоящий *Порт источника* TCP. Эти два значения вставляются в пакет. Затем заново подсчитываются контрольные суммы TCP и IP. Пакет передается на главный маршрутизатор компании для нормальной доставки с адресом вида 10.x.y.z.

АНАЛОГИЯ С ТЕЛЕФОННЫМ ДИСПЕТЧЕРОМ

- У компании есть один общий телефонный номер. Когда люди набирают его, они слышат голос оператора, который спрашивает, с кем именно они хотели бы соединиться, и подключают их к соответствующему добавочному телефонному номеру. Основной телефонный номер является аналогией IP-адреса компании, а добавочные на обоих концах аналогичны портам. Для адресации портов используется 16-битное поле, которое идентифицирует процесс, получающий входящий пакет.

КАК СЧИТАТЬ ДИАПАЗОНЫ

- перевод номера и маски подсети в двоичный вид
- По маске определить количество бит, предназначенных для адресации узлов (N) (ПОНЯТЬ ГДЕ НОМЕР ПОДСЕТИ, а ГДЕ НОМЕР УЗЛА)
- Общее количество адресов равно 2^N
- Начальный адрес: в номере узла все нули
- Конечный адрес: в номере узла все единицы