Сети ЭВМ и телекоммуникации

Лекция 8.

Глобальные сети.

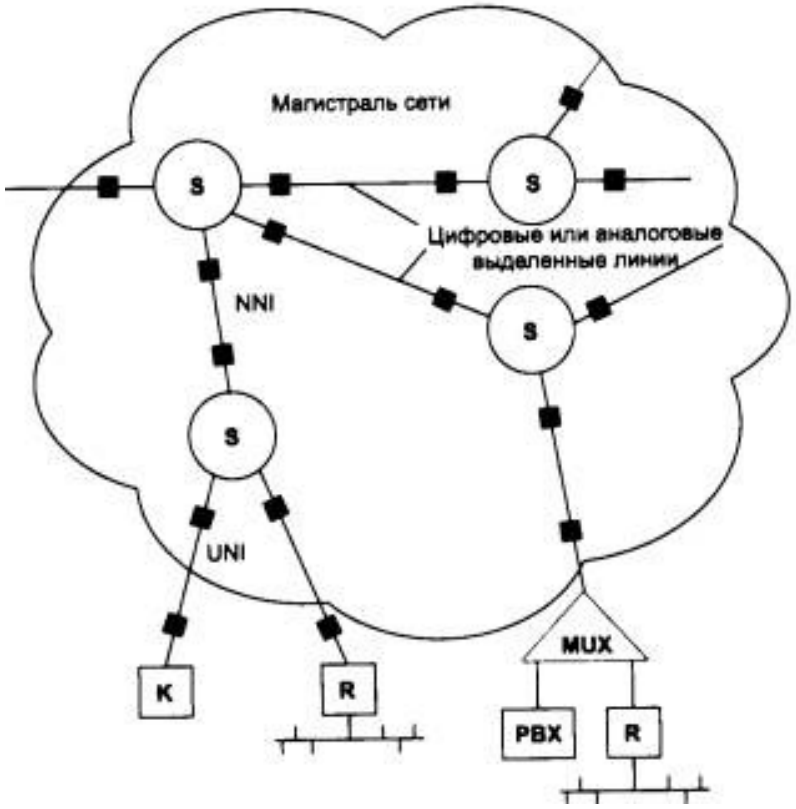
Технология NAT

Определение

- ***Глобальные сети*** *(Wide Area Networks, WAN)*, которые также называют территориальными компьютерными сетями, служат для того, чтобы предоставлять свои сервисы большому количеству конечных абонентов, разбросанных по большой территории - в пределах области, региона, страны, континента или всего земного шара
- Типичными абонентами глобальной компьютерной сети являются локальные сети предприятий, расположенные в разных городах и странах, которым нужно обмениваться данными между собой

Абоненты глобальной сети

Структура глобальной сети



- **S (switch)** – коммутаторы
- **K** - компьютеры
- **R (router)** – маршрутизаторы
- **MUX** - мультиплексор
- **PBX** – офисная АТС
- **UNI** (User-Network Interface) - интерфейс пользователь - сеть
- **NNI** (Network-Network Interface) - интерфейс сеть - сеть

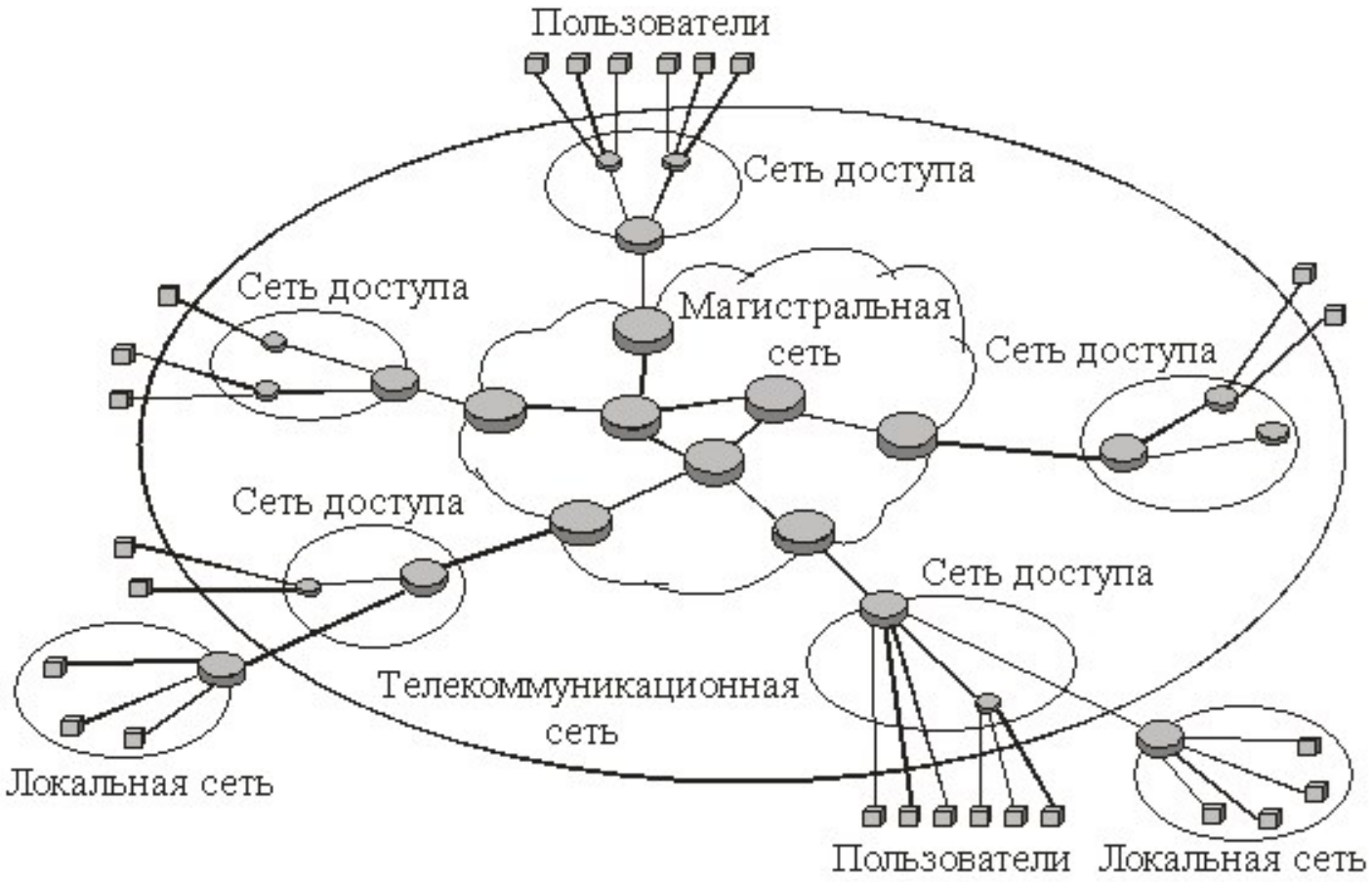
Особенности глобальных сетей

- **Глобальные компьютерные сети (WAN)** используются для объединения абонентов разных типов: отдельных компьютеров разных классов - от мэйнфреймов до персональных компьютеров, локальных компьютерных сетей, удаленных терминалов
- Ввиду большой стоимости инфраструктуры глобальной сети существует острая потребность передачи по одной сети **всех типов трафика**
- Глобальные сети предоставляют в основном транспортные услуги, транзитом перенося данные между локальными сетями или компьютерами
- Глобальные сети делятся на **магистральные сети** и **сети доступа**

Задачи глобальной сети

- Перенос данных из одной локальной сети в другую
- Web-узлы с большим количеством перекрестных ссылок
- Широковещательное распространение звукозаписей
- Организация интерактивных бесед
- Организация конференций
- Поиск информации

Типы глобальных сетей



Типы глобальных сетей

- **Магистральные сети** – используются для образования одноранговых связей между крупными локальными сетями
- **Сети доступа** – территориальные сети, необходимые для связи небольших локальных сетей и отдельных удаленных компьютеров с центральной локальной сетью

Технологии глобальных сетей

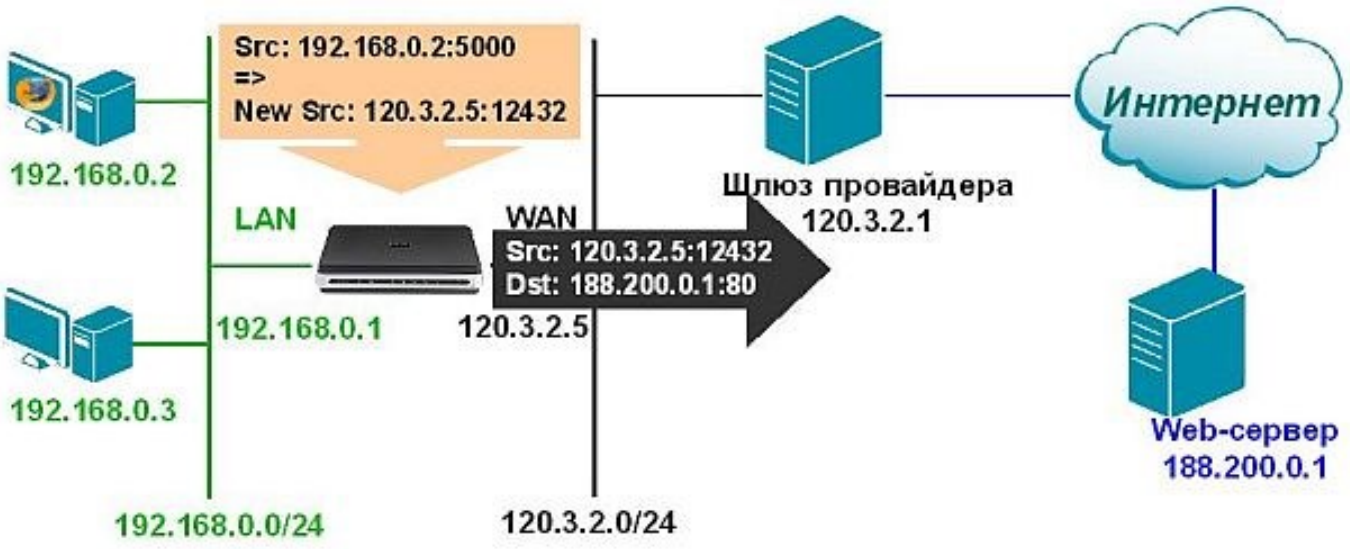
Тип сети	Скорость доступа	Трафик
X.25	1,2 – 64 Кбит/с	Терминальный
Frame Relay	64 Кбит/с – 2 Мбит/с	Компьютерный
SMDS	1,544– 45 Мбит/с	Компьютерный, графика, голос, видео
ATM	1,544– 155 Мбит/с	Компьютерный, графика, голос, видео
TCP/IP	1,2 Кбит/с – 2 Мбит/с	Терминальный, компьютерный

Технология преобразования сетевых адресов (NAT)

- **NAT** (Network Address Translation – преобразование сетевых адресов) – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Механизм NAT описан в RFC 1631, RFC 3022
- Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством – Интернет-маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является **Source NAT** (**SNAT**), суть механизма которого состоит в замене адреса источника (**source**) при прохождении пакета в одну сторону и обратной замене адреса назначения (**destination**) в ответном пакете. Наряду с адресами источника/назначения могут также заменяться номера портов источника и назначения

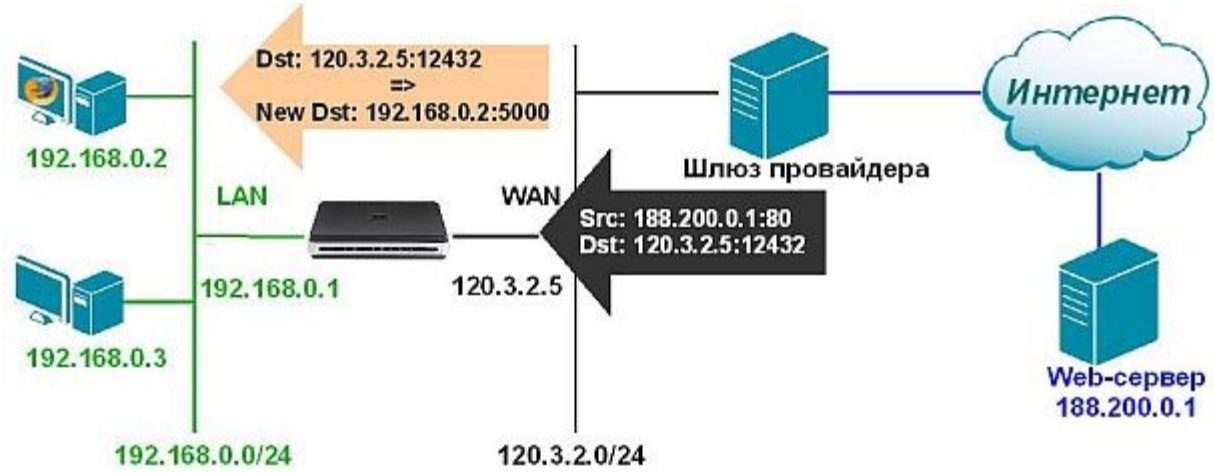
Структура NAT

Преобразование адреса



- Устройство NAT получает пакет и делает запись в таблице отслеживания соединений, которая управляет преобразованием адресов
- Затем подменяет адрес источника пакета собственным внешним общедоступным IP-адресом и посылает пакет по месту назначения в Интернет

Принятие запроса



- Устройство NAT, получив ответ, отыскивает отправителя исходного пакета в таблице отслеживания соединений, заменяет IP-адрес назначения на соответствующий частный IP-адрес и передает пакет на исходный компьютер. Поскольку устройство NAT посылает пакеты от имени всех внутренних компьютеров, оно изменяет исходный сетевой порт и данная информация хранится в таблице отслеживания соединений

Три базовых концепции NAT

- **статическая (SAT, Static Network Address Translation)** - отображает локальные IP-адреса на конкретные публичные адреса на основании один к одному. Применяется, когда локальный хост должен быть доступен извне с использованием фиксированных адресов
- **динамическая (DAT, Dynamic Address Translation)** - отображает набор частных адресов на некое множество публичных IP-адресов. Если число локальных хостов не превышает число имеющихся публичных адресов, каждому локальному адресу будет гарантироваться соответствие публичного адреса. В противном случае, число хостов, которые могут одновременно получить доступ во внешние сети, будет ограничено количеством публичных адресов
- **маскарадная** (**NAPT, NAT Overload, PAT**) - форма динамического NAT, который отображает несколько частных адресов в единственный публичный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation)

Четыре типа трансляции

Механизмов взаимодействия внутренней локальной сети с внешней общедоступной сетью может быть несколько – это зависит от конкретной задачи по обеспечению доступа во внешнюю сеть и обратно и прописывается определенными правилами. Определены 4 типа трансляции сетевых адресов:

- **Full Cone** (Полный конус)
- **Restricted Cone** (Ограниченный конус)
- **Port Restricted Cone** (Порт ограниченного конуса)
- **Symmetric** (Симметричный)

В первых трех типах NAT для взаимодействия разных IP-адресов внешней сети с адресами из локальной сети используется один и тот же внешний порт. Четвертый тип – симметричный – для каждого адреса и порта использует отдельный внешний порт

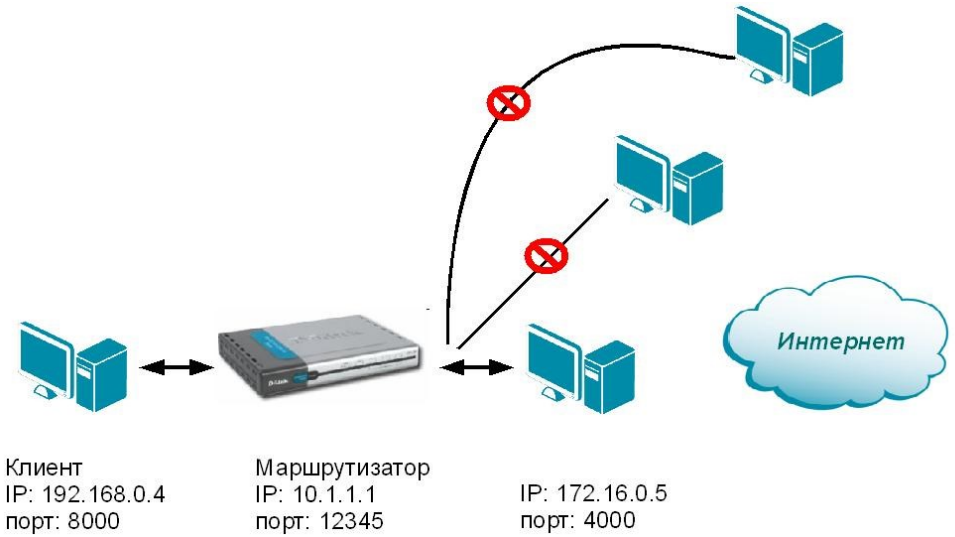
NAT Full Cone

Внешний порт устройства открыт для приходящих с любых адресов запросов. Если пользователю из Интернета нужно отправить пакет клиенту, расположенному за NAT'ом, то ему необходимо знать только внешний порт устройства, через который установлено соединение.
Например, компьютер за NAT'ом с IP-адресом **192.168.0.4** посылает и получает пакеты через порт **8000**, которые отображаются на внешний IP-адрес и порт, как **10.1.1.1:12345**. Пакеты из внешней сети приходят на устройство с IP-адресом **10.1.1.1:12345** и далее отправляются на клиентский компьютер **192.168.0.4:8000**

NAT Restricted Cone

Внешний порт устройства открыт для любого пакета, посланного с клиентского компьютера, в нашем примере: **192.168.0.4:8000**. А пакет, пришедший из внешней сети (например, от компьютера **172.16.0.5:4000**) на устройство с адресом **10.1.1.1:12345**, будет отправлен на компьютер **192.168.0.4:8000** только в том случае, если **192.168.0.4:8000** предварительно посылал запрос на IP-адрес внешнего хоста (в нашем случае – на компьютер **172.16.0.5:4000**). То есть, маршрутизатор будет транслировать входящие пакеты только с определенного адреса источника (в нашем случае компьютер **172.16.0.5:4000**), но номер порта источника при этом может быть любым.

В противном случае, NAT блокирует пакеты, пришедшие с хостов, на которые **192.168.0.4:8000** не отправлял запроса



NAT Port Restricted Cone

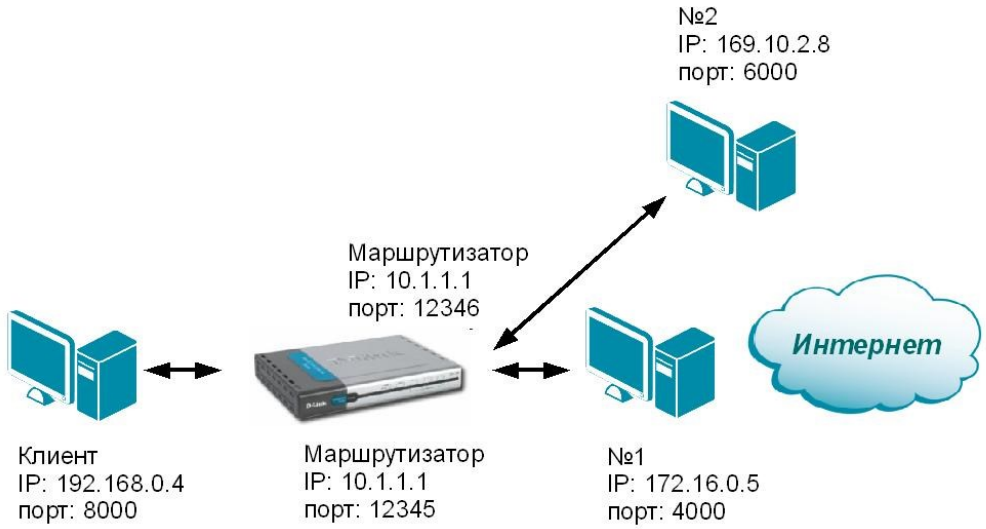
Механизм NAT Port Restricted Cone почти аналогичен механизму NAT Restricted Cone. Только в данном случае NAT блокирует все пакеты, пришедшие с хостов, на которые клиентский компьютер **192.168.0.4:8000** не отправлял запроса по какому-либо IP-адресу и порту. Маршрутизатор обращает внимание на соответствие номера порта источника и не обращает внимания на адрес источника. В нашем примере маршрутизатор будет транслировать входящие пакеты с любым адресом источника, но порт источника при этом должен быть 4000. Если клиент отправил запросы во внешнюю сеть к нескольким IP-адресам и портам, то они смогут посылать пакеты клиенту на IP-адрес:порт **10.1.1.1:12345**

Symmetric NAT

Symmetric NAT отличается от первых трех механизмов способом отображения внутреннего IP-адреса:порта на внешний адрес:порт. Это отображение зависит от IP-адреса:порта компьютера, которому предназначен посланный запрос. Например, если клиентский компьютер **192.168.0.4:8000** посылает запрос компьютеру №1 (**172.16.0.5:4000**), то он может быть отображен как **10.1.1.1:12345**, в тоже время, если он посылает с того же самого порта (**192.168.0.4:8000**) на другой IP-адрес, он отображается по-другому (**10.1.1.1:12346**).

Компьютер №1 (172.16.0.5:4000) может отправить пакет только на 10.1.1.1:12345

Компьютер №2 (169.10.2.8:6000) – только на 10.1.1.1:12346. Если любой из них попытается отправить пакеты на порт, с которого он не получал запроса, NAT заблокирует данные пакеты



Функции NAT

1. Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с частными (внутренними) IP-адресами
2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения из внутренней сети во внешнюю. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих из внешней сети, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются
3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов

Недостатки технологии NAT

1. Не все протоколы могут "преодолеть" NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Опеределенные межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP)
2. Из-за трансляции адресов "много в один" появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций
3. Атака DoS со стороны узла, осуществляющего NAT – если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений