Информационные технологии корпоративных сетей

Преподаватель: **ГУБИН Александр Николаевич**

к.т.н., доц.

каф. ИУС (ауд. 631) Тел. 3051278

Информационные технологии корпоративных сетей

Состав курса (9-ый сем):

Лекции - 22 ч.

Лаб.р. - 8 ч.

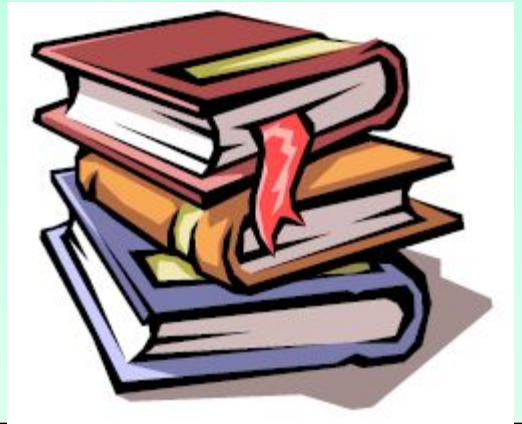
Кпр.

Экзамен

Лекция №1

Литература:

1. Э.Таненбаум, Д.Уэзеролл. Компьютерные сети. 5-е издание, Питер, 2012, 955 с.
2. Ломовицкий В.В. И др. Основы построения систем и сетей передачи информации: Учебное пособие для вузов. М.: Горячая линия-Телеком, 2005.-382с.



Информационные технологии корпоративных сетей

Лекция № 1 (2 ч)

- Предмет и задачи дисциплины.
- Корпоративные сети. Основные понятия.
- Трансляция адресов. Основные задачи.
- Особенности организации трансляции адресов
- Основные схемы трансляции адресов
- Реализация трансляции адресов

Предмет и задачи дисциплины

Предметом изучения дисциплины являются **информационные технологии корпоративных сетей** – как объекты разработки, исследования и проектирования.

Процесс изучения дисциплины направлен на формирование таких компетенций как способность к использованию современных информационных технологий и полученных знаний в своей предметной области.

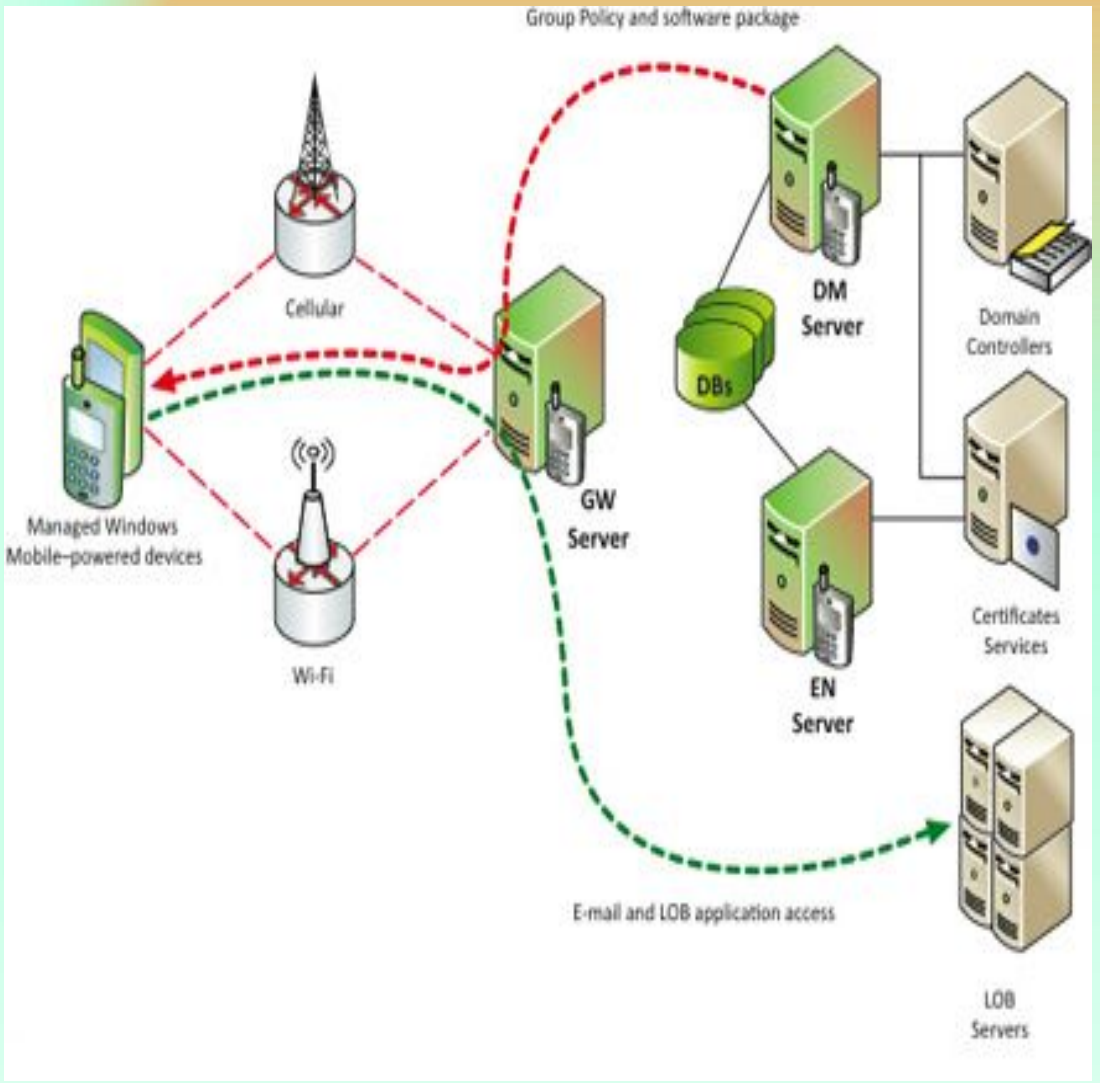
Результатом освоения дисциплины должно быть:
1. Формирование знаний об основных методах реализации и особенностей использования базовых информационных технологий в корпоративных сетях.

Предмет и задачи дисциплины

2.Формирования умения использовать полученные знания в процессе проектирования и эксплуатации ИС.

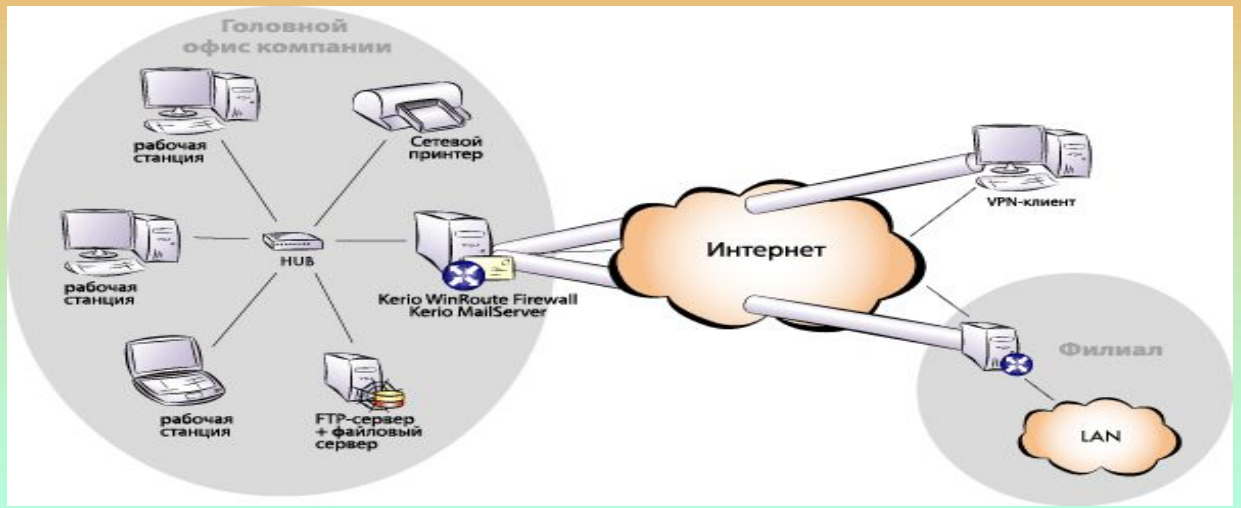
Кроме того, после изучения данной дисциплины каждый студент должен владеть методами реализации базовых информационных технологий в составе корпоративных сетей.

Корпоративные сети. Основные понятия.



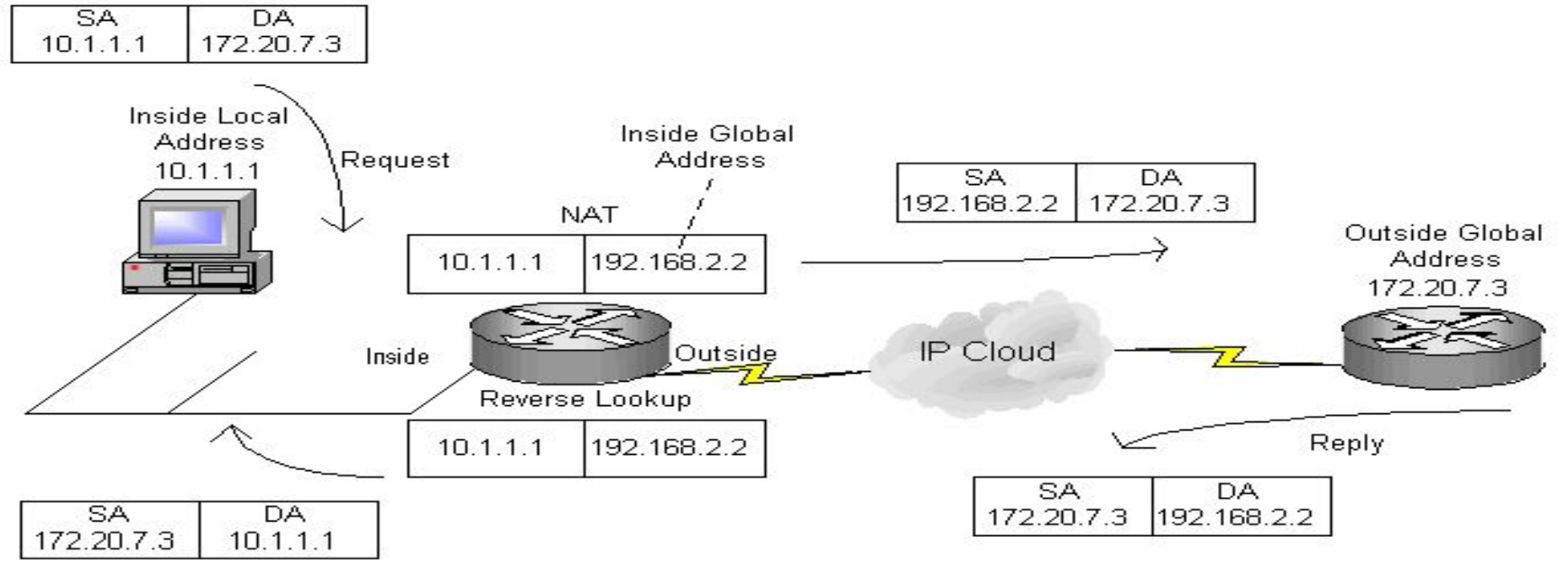
Корпоративная сеть – это информационно-коммуникационная система, принадлежащая и управляемая организацией в соответствии с правилами этой организации.

Корпоративные сети. Основные понятия.



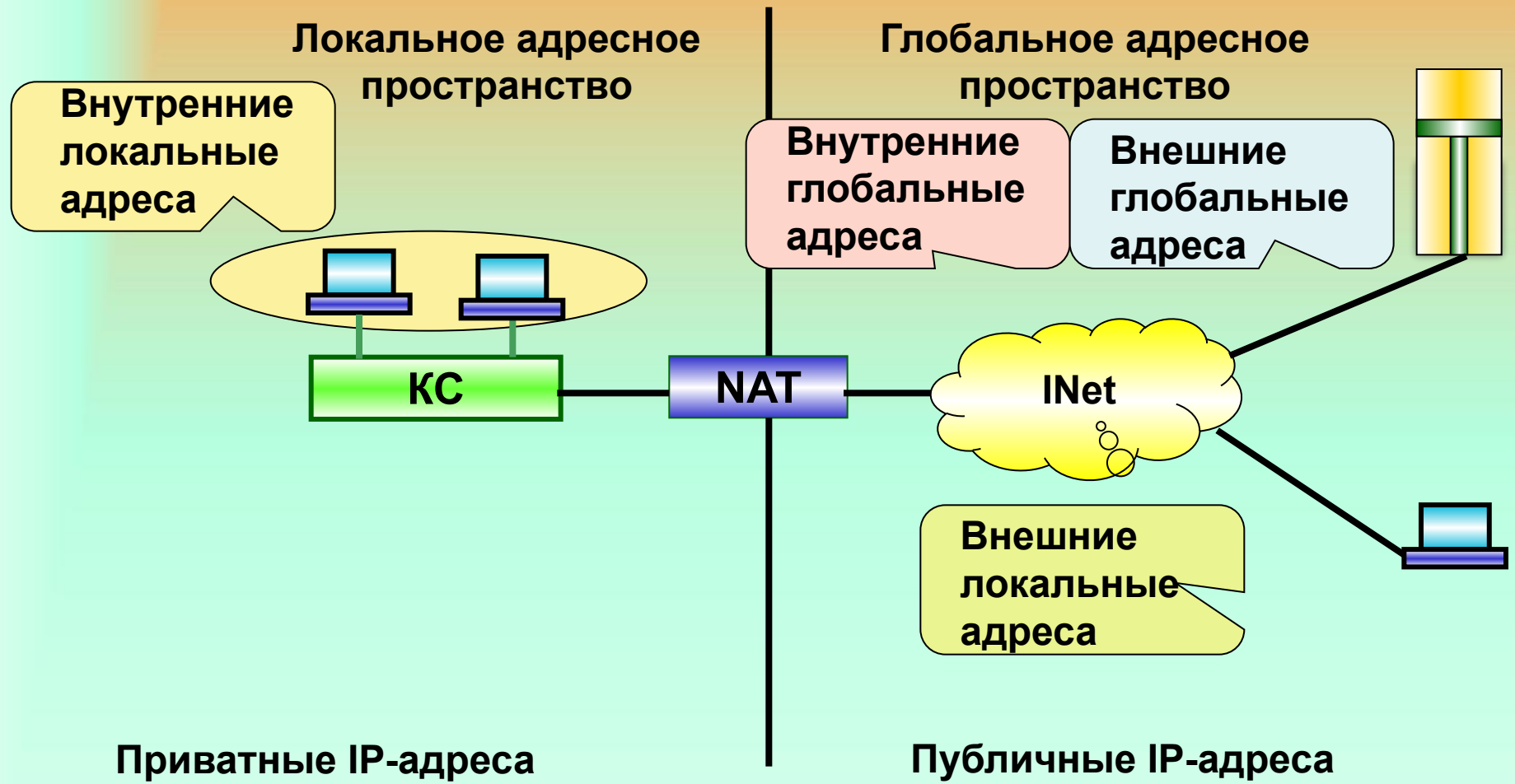
Корпоративная сеть (КС) отличается от иных тем, что правила распределения IP адресов, работы с интернет ресурсами и др. едины для всей КС. Провайдер, например, контролирует только магистральный сегмент своей сети, позволяя своим клиентам самостоятельно управлять сетью внутри КС.

Корпоративные сети. Основные понятия.

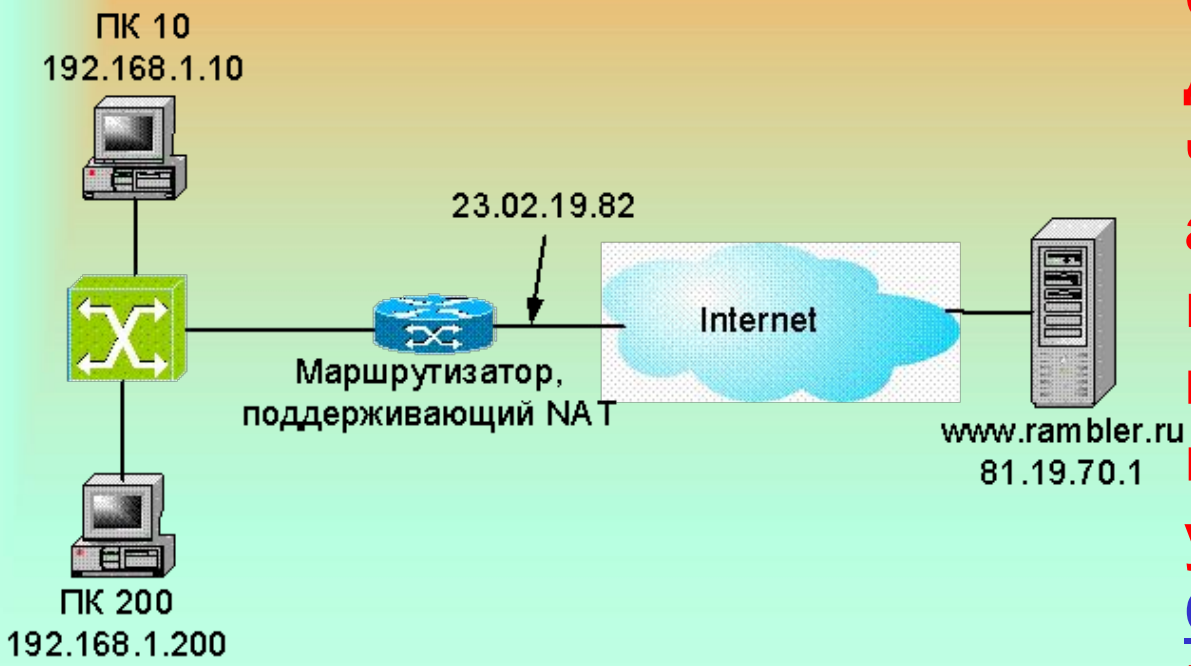


Адресное пространство КС, как правило скрыто от провайдера механизмом трансляции адресов - NAT (Network Address Translation)

Корпоративные сети. Определения IP-адресов.



Трансляция адресов. Основные задачи..



10.0.0.0 -10.255.255.255/8 (16 777 216 хостов)

172.16.0.0 – 172.31.255.255/12 (1 048 576 хостов)

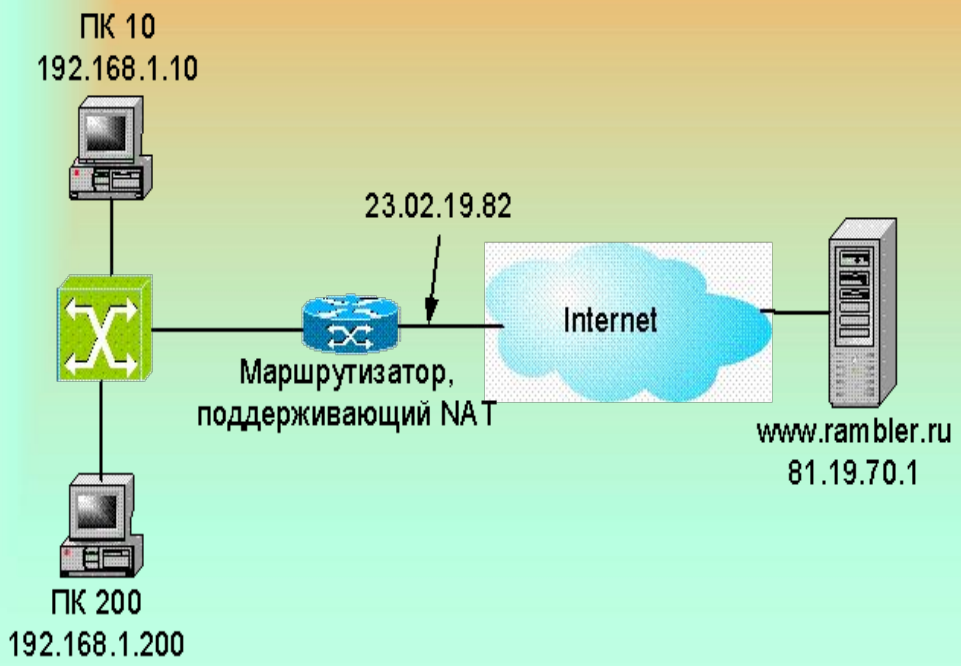
192.168.0.0 – 192.168.255.255/16 (65 536 хостов)

Существует три диапазона частных IP-адресов. Они могут использоваться внутри сети по ее усмотрению.

Ограничение.

Пакеты с такими адресами не должны появляться во внешней сети (в интернете).

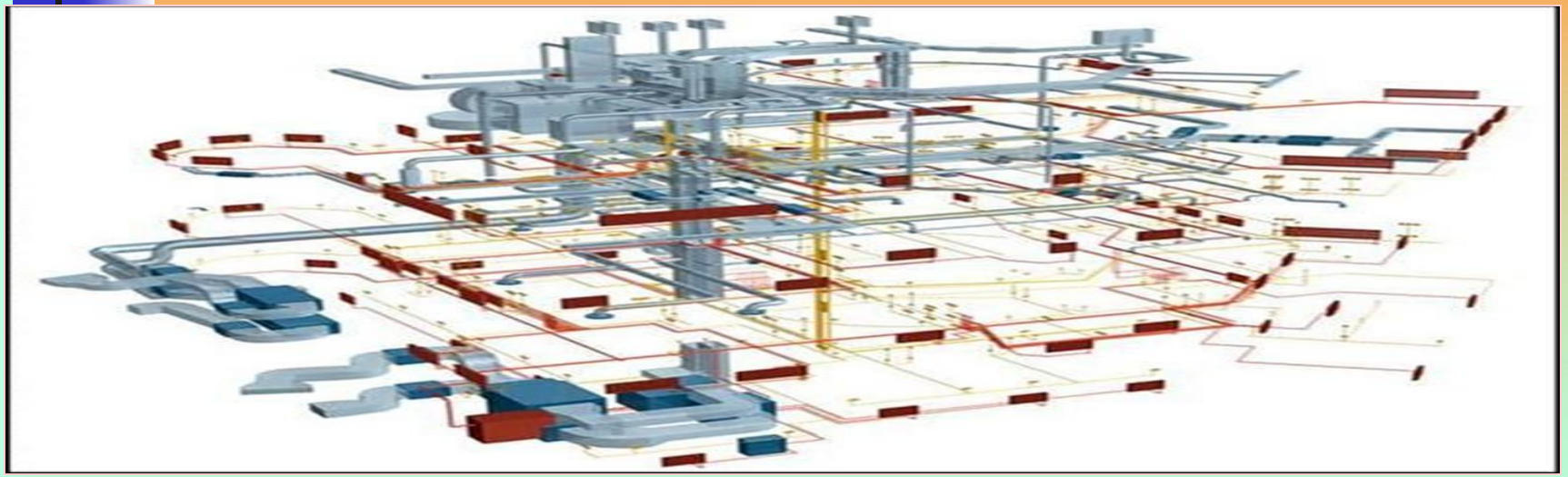
Трансляция адресов. Основные задачи..



Уникальность внешних IP адресов достигается тем, что они выдаются централизованно Сетевым Информационным Центром (Network Information Center – NIC)

ARIN (Северная Америка)
RIPE NCC (Европа, часть Азии)
APNIC (Азия, Тихоокеанский регион)
LACNIC (Латинская Америка и Карибский регион)
AfriNIC (Африка)

Трансляция адресов. Основные задачи..



Внутри КС каждый компьютер получает уникальный IP-адрес, который используется для маршрутизации внутреннего трафика.

Когда пакет покидает КС, производится трансляция адреса, при котором внутренний IP-адрес становится публичным IP-адресом

Трансляция адресов. Основные задачи..

ВымпелКом
217.118.80.0 - 217.118.83.255
JSC "VimpelCom" WLAN1 Moscow
217.118.84.0 - 217.118.87.255
BEEOFFICE, JSC "VimpelCom" Russia
89.188.224.0 - 89.188.227.255
Sakhalin Telecom network, RU
217.118.92.0 - 217.118.95.255
JSC
83.220.224.0 - 83.220.227.255
Region1, GPRS in regions, JSC "VimpelCom"
217.118.76.0 - 217.118.79.255
BEEGPRSPE, JSC "VimpelCom" GPRS_SPbE Russia

МегаФон
193.201.228.0 - 193.201.231.255
Network for Sonic Duo, Moscow
85.26.160.0 - 85.26.163.255
OJSC MSS-Povolzhe network - GPRS Access Pool No. 2, RU
85.26.176.0 - 85.26.179.255
CJSC Mobicom-Kavkaz network (Part 3), RU
83.149.9.19 - 83.149.11.255
MF-MOSCOW, Customers Dynamic VPN Access, RU
85.26.224.0 - 85.26.227.255
CJSC Mobicom-Novosibirsk additional network., RU
83.149.32.0 - 83.149.35.255
CJSC Uralsky GSM network
85.26.148.0 - 85.26.151.255
OJSC MSS-Povolzhe network - GPRS Access Pool No. 3, RU

Трансляция адресов. Основные задачи..

6.* – Army Information Systems Center
7.*.*.* Defense Information Systems Agency, VA

128.56.0.0 U.S. Naval Academy
128.60.0.0 Naval Research Laboratory
128.63.0.0 Army Ballistics Research Laboratory
128.80.0.0 Army Communications Electronics Command
128.98.0.0 – 128.98.255.255 Defence Evaluation and Research Agency
128.102.0.0 NASA Ames Research Center
128.149.0.0 NASA Headquarters
128.154.0.0 NASA Wallops Flight Facility
128.155.0.0 NASA Langley Research Center
128.156.0.0 NASA Lewis Network Control Center
128.217.0.0 NASA Kennedy Space Center
128.236.0.0 U.S. Air Force Academy
137.5.0.0 Air Force Concentrator Network
137.6.0.0 Air Force Concentrator Network
137.11.0.0 HQ AFSPC/SCNNC
137.12.0.0 Air Force Concentrator Network
137.17.* National Aerospace Laboratory

Трансляция адресов. Основные задачи..

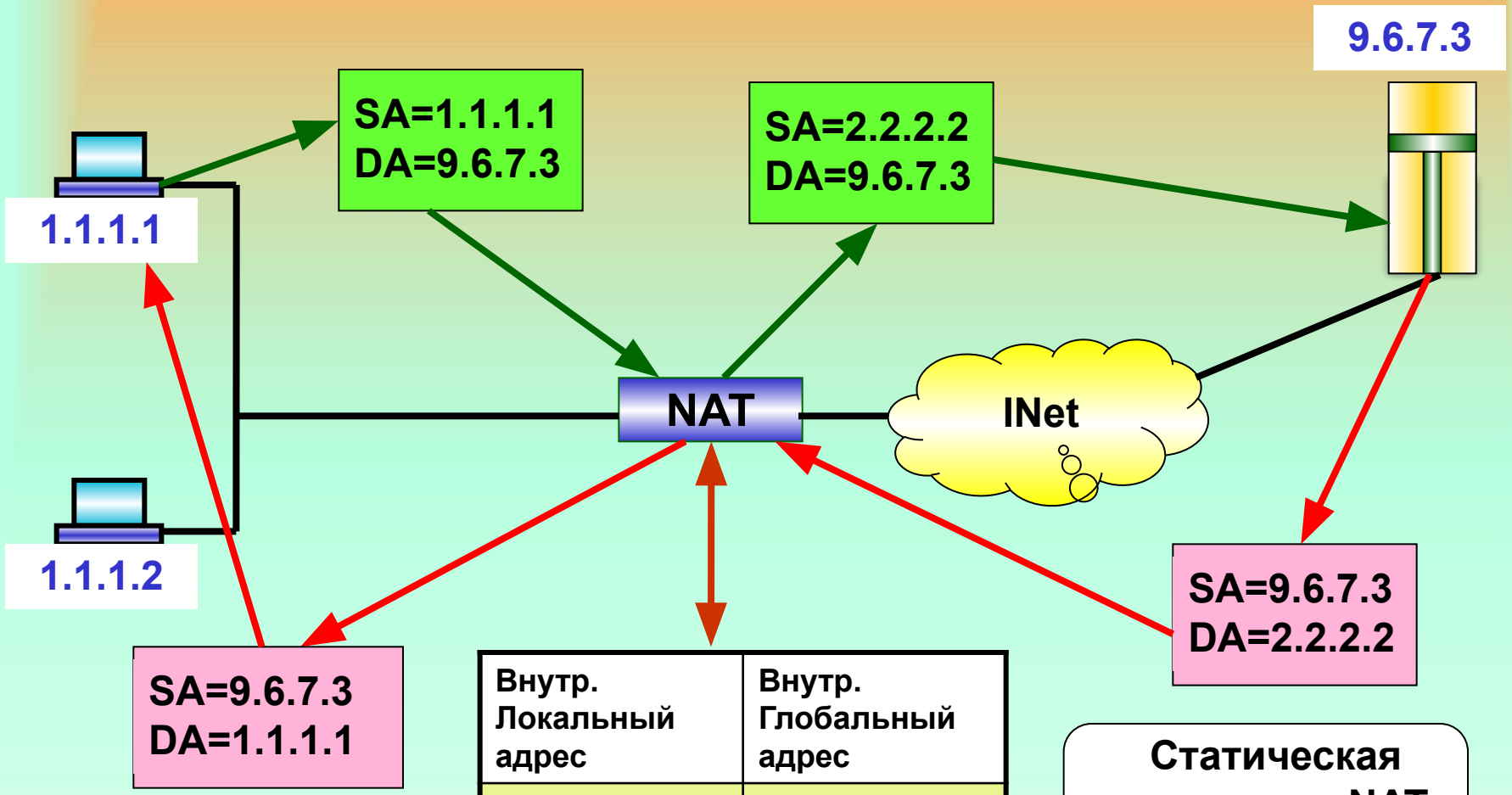
Основная причина появления NAT (Network Address Translation) - дефицит public IP-адресов.

Существуют:

- **Статический NAT**
- **Динамический NAT**
- **Перегруженный NAT**
- **NAT перекрывающийся адресов**
- **NAT для распределения нагрузки**

Корпоративные сети. Статический NAT.

1 внутренний локальный IP ⟺ **1 внешний глобальный IP**

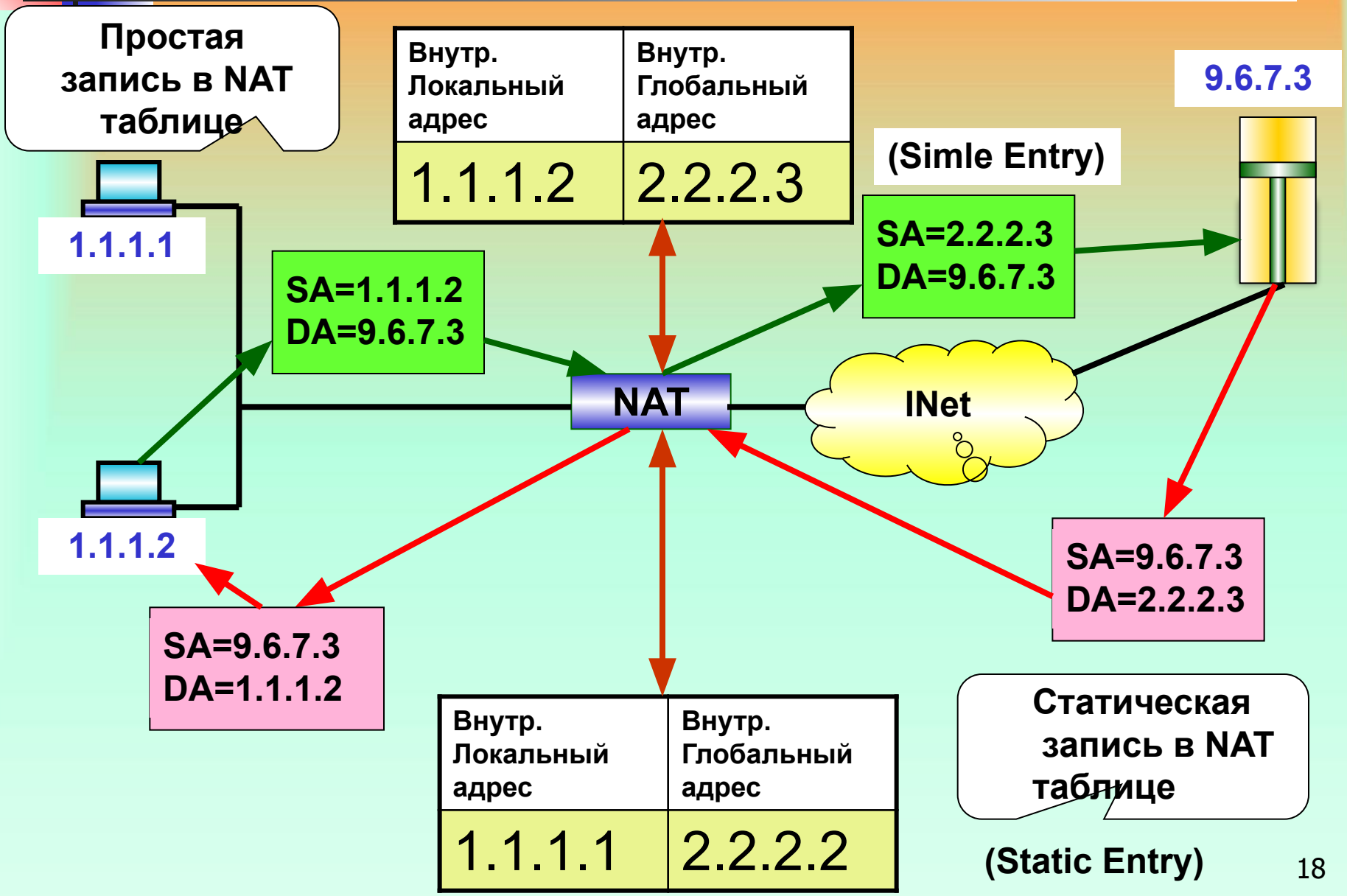


Внутр. Локальный адрес	Внутр. Глобальный адрес
1.1.1.1	2.2.2.2

Статическая запись в NAT таблице

(Static Entry)

Корпоративные сети. Динамический NAT.



Трансляция адресов. Конфигурирование оборудования для статической трансляции(Cisco)

Действие	Команда
Установить режим статической трансляции между внутренним локальным адресом и внутренним глобальным адресом	ip nat inside source static <локальный адрес> <глобальный адрес>
Указать внутренний интерфейс	interface <тип> <номер>
Пометить данный интерфейс, как принадлежащий внутренней сети	ip nat inside
Указать внешний интерфейс	interface <тип> <номер>
Пометить данный интерфейс, как принадлежащий внешней сети	ip nat outside

При использовании нескольких внутренних и внешних интерфейсов необходимо аналогичные действия произвести и в отношении остальных интерфейсов.

Трансляция адресов. Конфигурирование оборудования для динамической трансляции (Cisco)

Действие	Команда
Определить пул глобальных адресов	ip nat pool <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]
Определить стандартный список доступа, регламентирующий адреса, подлежащие трансляции	access-list <номер> permit <адрес или блок адресов>
Установить динамическую трансляцию на основе списка доступа, определенного на предыдущем шаге	ip nat inside source list <номер списка доступа> pool <имя>
Указать внутренний интерфейс	interface <тип> <номер>
Пометить данный интерфейс, как принадлежащий внутренней сети	ip nat inside
Указать внешний интерфейс	interface <тип> <номер>
Пометить данный интерфейс, как принадлежащий внешней сети	ip nat outside

Трансляция адресов. Конфигурирование оборудования ПРИМЕР

Осуществляется трансляция всех адресов узлов-источников, определенных списком доступа 1 (разрешены адреса от 192.168.1.0/24), в пул адресов, названный net-208. Этот пул содержит адреса с 171.69.233.208 по 171.69.233.233.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask 255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0 ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1. 0 0.0.0.255
```

Трансляция адресов. Использование одного глобального адреса (маскарадинг)

N внутренних локальных IP  1 внешний глобальный IP

Технология трансляции предусматривает использование информации протоколов более высокого уровня (транспортный уровень). TCP –Transmition Control Protocol (протокол управления передачей) и UDP - User Datagram Protocol (протокол пользовательских дейтаграмм), которые содержат номера портов.

Номера портов используют для корректного решения задачи соответствия нескольких внутренних локальных адресов одному глобальному адресу (номера портов связаны с внутренним локальным адресом)

Трансляция адресов. Номер порта.

Номер порта (в TCP и UDP) – это системный ресурс, который идентифицируется номером и выделяется приложению, выполняемому на некотором сетевом хосте для связи с приложениями, выполняемыми на других сетевых хостах.

Компьютер (поддерживающий TCP) содержит в составе ОС транспортную подсистему (библиотечная процедура, часть ядра или процесс пользователя). В основе работы этой подсистемы лежит понятие сокетов (Беркли) – (гнездо, конечная точка). У каждого сокета есть адрес, который состоит из IP адреса хоста и 16- битного номера (локального относительно хоста). Этот 16- битный номер и получил название порта.

Трансляция адресов. Номер порта.

Номера портов выбираются по требованию приложений. В выборе номеров портов существует определенный порядок.
Порты с номерами ниже 1024 зарезервированы стандартными сервисами и доступны только привилегированным пользователям. Эти порты получили название well-known ports (известные порты). Список известных портов можно посмотреть на сайте WWW.IANA.ORG

Порты с 1024 по 49151 можно зарегистрировать через IANA . Но обычно с выбором портов по требованиям приложений справляется ОС

Трансляция адресов. Номер порта.

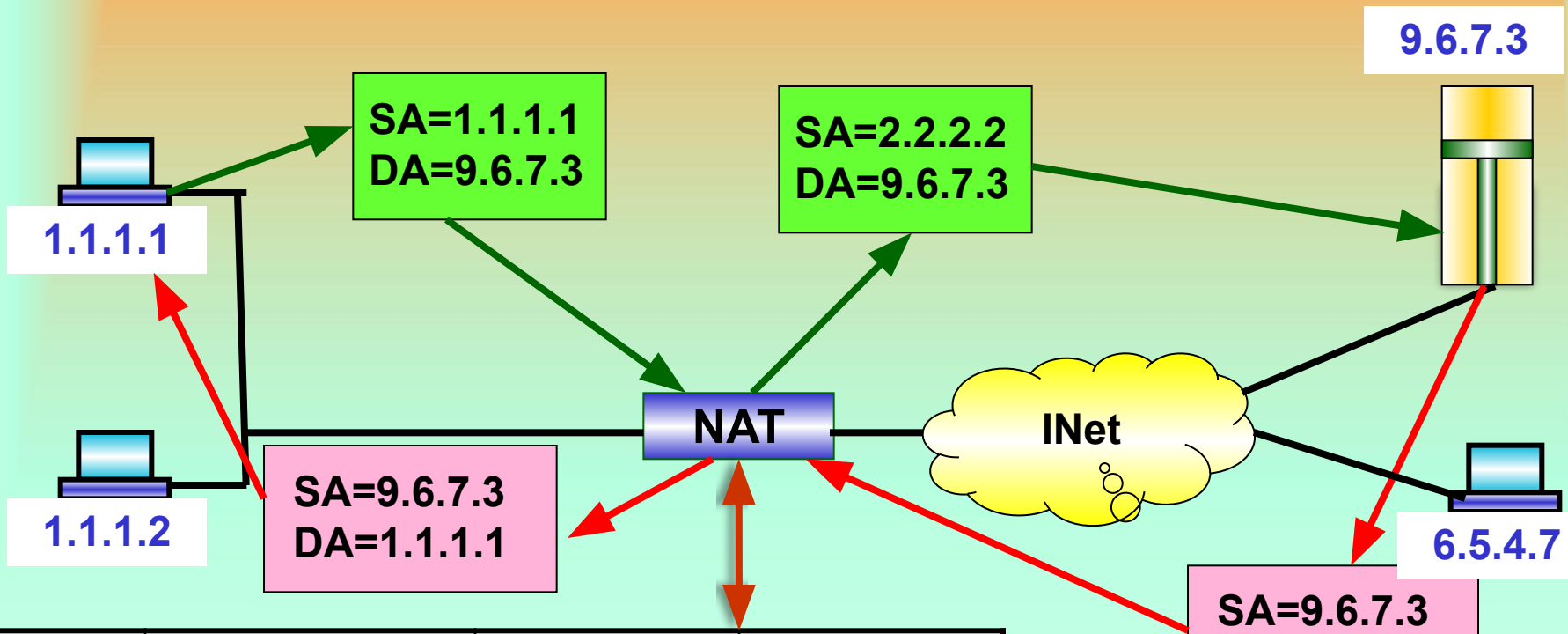
ПОРТ	ПРОТОКОЛ	ИСПОЛЬЗОВАНИЕ
20, 21	FTP	Передача файлов
25	SMTP	Электронная почта
80	HTTP	WWW (интернет)
110	POP-3	Удаленный доступ к электронной почте

Трансляция адресов. Маскарадинг

В качестве критерия принадлежности пакета определенному внутреннему локальному адресу используется номер порта из протокола более высокого уровня (транспортного).

Корпоративные сети. Маскарадинг.

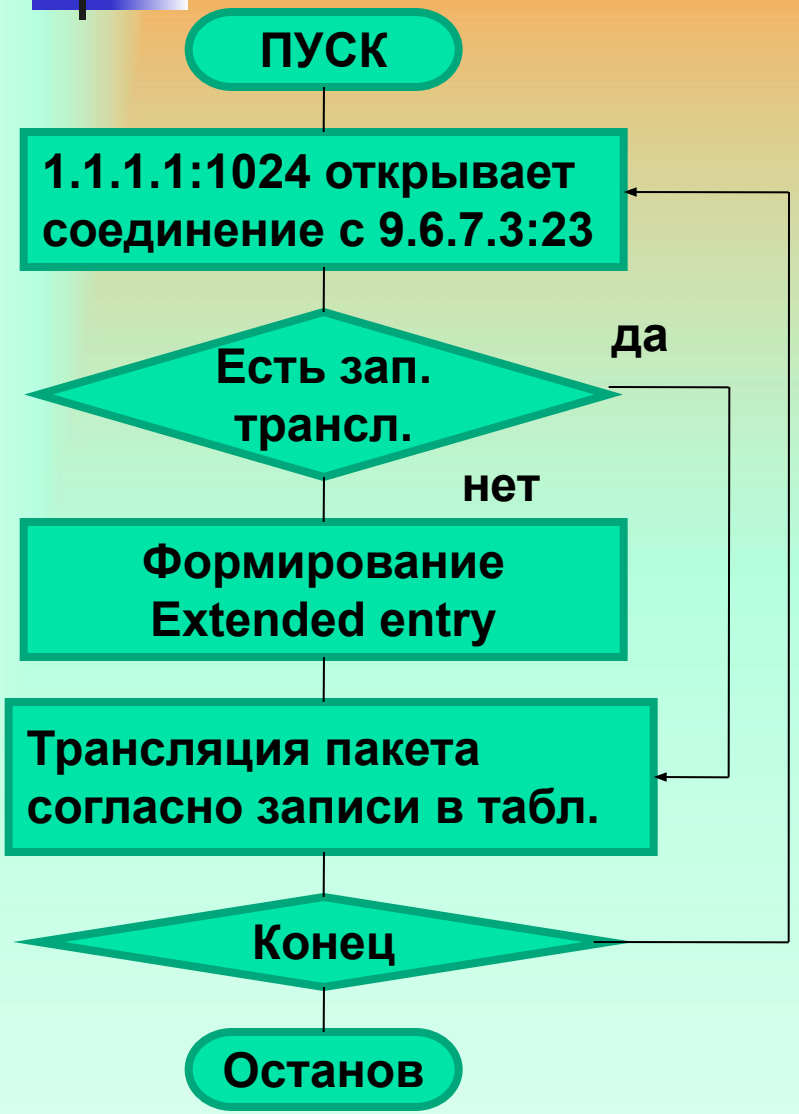
N внутренних локальных IP ⟺ **1 внешний глобальный IP**

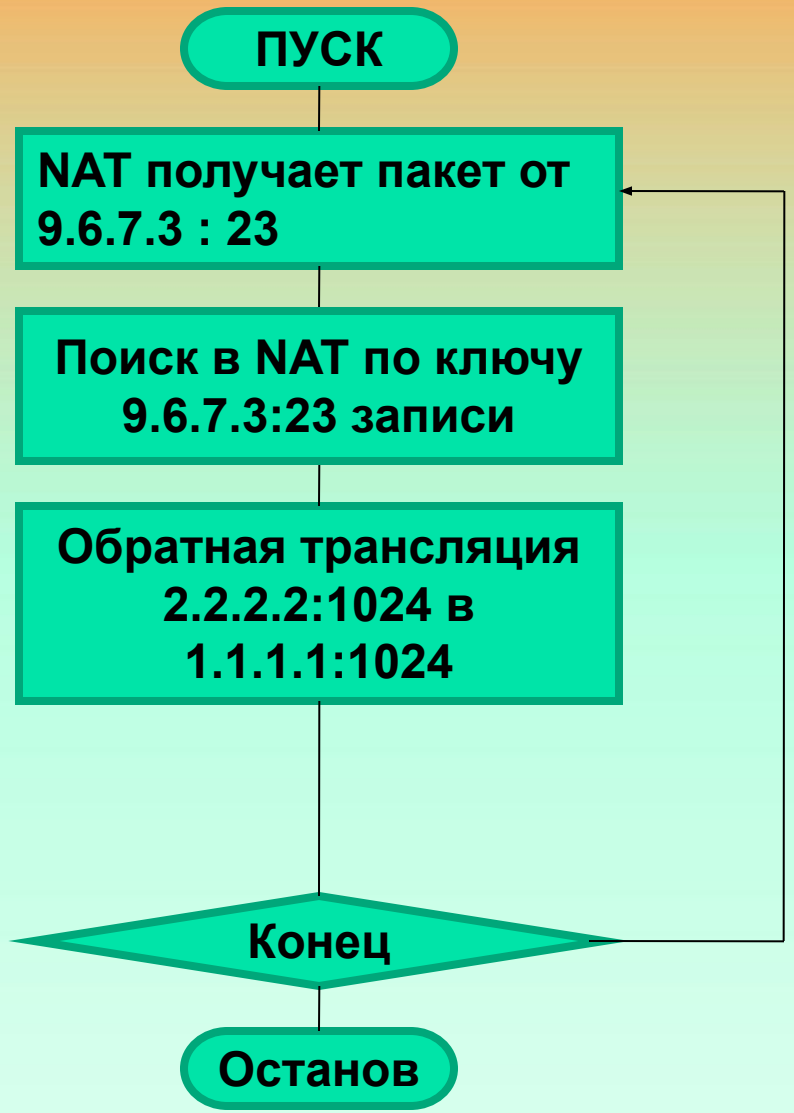


Протокол	Внутр. Локальный адрес	Внутр. Глобальный адрес	Внешний Глобальный адрес
TCP	1.1.1.1 :1024	2.2.2.2 : 1024	9.6.7.3 : 23
TCP	1.1.1.2 : 1723	2.2.2.2 : 1723	6.5.4.7 : 80

Extended Entry

Корпоративные сети. Маскарадинг.





Корпоративные сети. Маскарадинг.

Пример: доступ локальных пользователей в Internet посредством Overload (PAT)

PAT (Port Address Translation) — трансляция адресов портов.

```
interface ethernet 0
ip address 10.10.10.1 255.255.255.0
ip nat inside

!--- Настройка IP-адреса для Ethernet 0 и использование в качестве внутреннего
NAT интерфейса.


interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Настройка IP-адреса для Ethernet 1 и использование в качестве внутреннего
NAT интерфейса.
```

Корпоративные сети. Маскарадинг.

Пример: доступ локальных пользователей в Internet посредством Overload (PAT)

```
interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Настройка IP-адреса для serial 0 и использование в качестве внешнего NAT интерфейса.


ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
!

!--- Конфигурирование NAT пула с именем ovrld с единственным IP-адресом, 172.16.10.1.
```

Корпоративные сети. Маскарадинг.

Пример: доступ локальных пользователей в Internet посредством Overload (PAT)

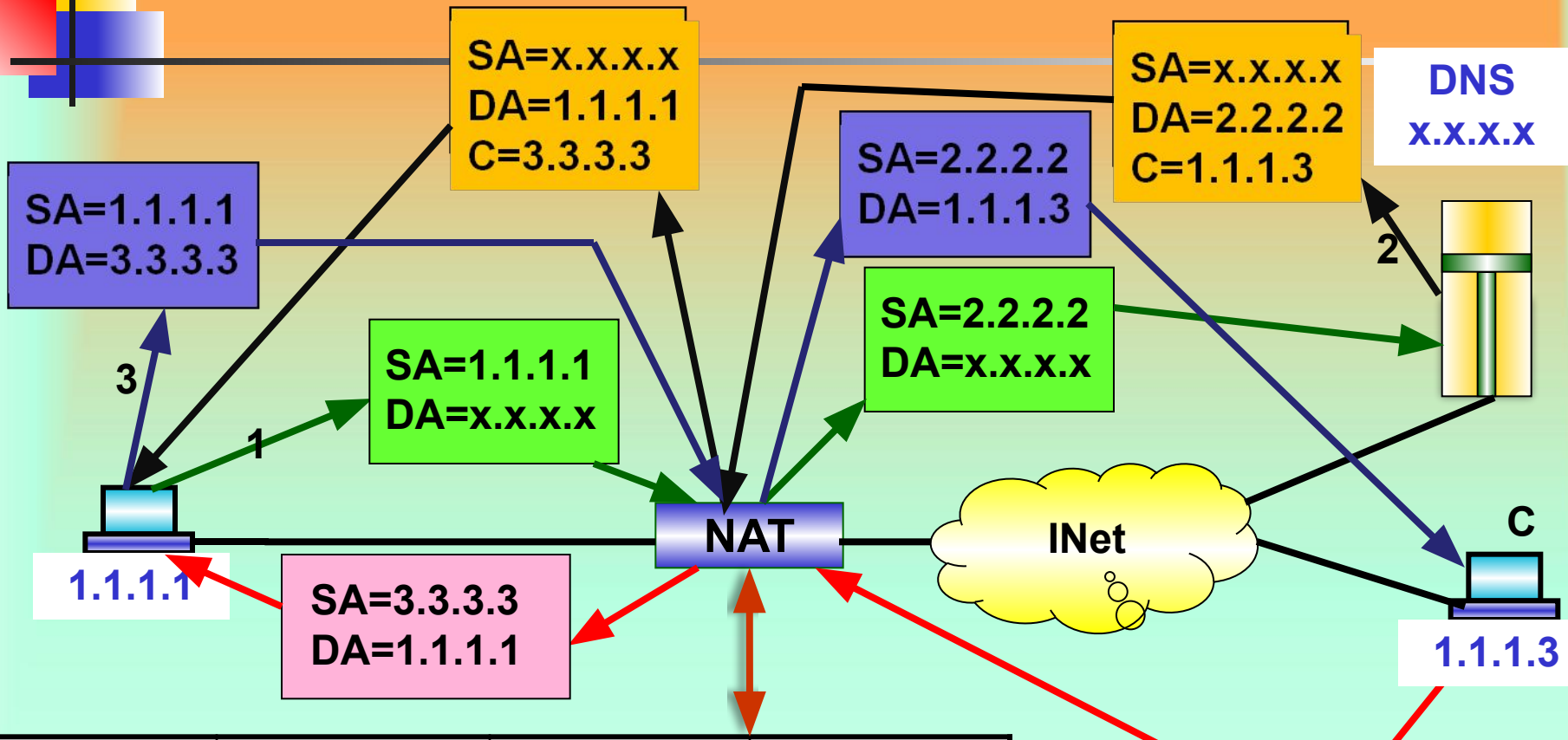
```
ip nat inside source list 7 pool ovrld overload
!

!--- Указание какие пакеты могут "проходить" через внутренний интерфейс,
разрешающий акл access-list 7 исходного адреса.
!--- Транслируется на внешний NAT пул с именем ovrld.
!--- Трансляции overloaded с разрешением нескольких внутренних устройств,
транслирующихся на определённый IP-адрес.


access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 разрешает пакеты с исходными адресами в диапазоне от
10.10.10.0 через 10.10.10.31 и 10.10.20.0 через 10.10.20.31.
```

Трансляция перекрывающихся адресов.

Используется в случаях, когда одна сеть использует адресное пространство другой сети и в то же время необходимо организовать взаимодействие этих сетей. Обычно используется динамический NAT с DNS сервером.

Ситуацию, когда один и тот же адрес используется как легальный и как нелегальный называют перекрытием (Overlapping)

Трансляция перекрывающихся адресов



Внутр. Локальный адрес	Внутр. Глобальный адрес	Внешний Глобальный адрес	Внешний Локальный адрес
1.1.1.1	2.2.2.2	1.1.1.3	3.3.3.3

Трансляция перекрывающихся адресов

- **Внутренний пользователь 1.1.1.1 открывает соединение с узлом C по имени, полученном от DNS сервера.**

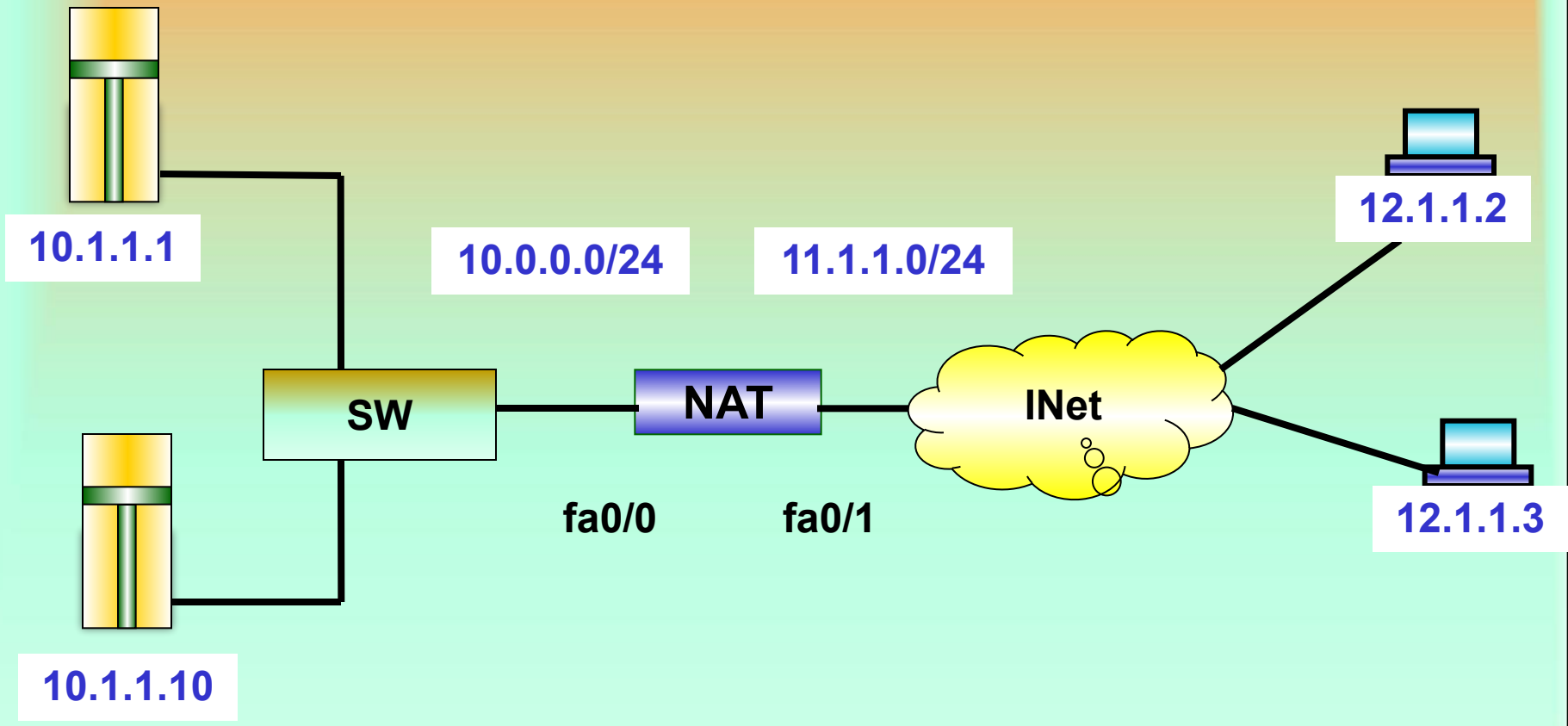
- **Маршрутизатор перехватывает ответ DNS и транслирует адрес перекрытия (1.1.1.3). Для обеспечения трансляции маршрутизатор создает простую запись трансляции, которая устанавливает связь между 1.1.1.3 и адресом 3.3.3.3 из предварительно сформированного пула внешних локальных адресов (внешние локальные адреса не могут находится во внутненней сети)**

- **Узел 1.1.1.1 открывает соединение с узлом 3.3.3.3**

Использование NAT для распределения нагрузки TCP

Используется для балансировки нагрузки между серверами. Данный вид трансляции является динамическим по своей природе. Есть десять серверов (10.0.0.1-10.0.0.10) на которых крутится один сайт (порт у них один и тот же -80). Необходимо сбалансировать нагрузку по алгоритму Round Robin
(следующий клиент, обращающийся по тому же адресу должен попадать на другой сервер)

Распределение нагрузки



Распределение нагрузки

РАБОТА

- **Прямая трансляция. outside –to- inside. При появлении TCP трафика на outside интерфейсе, трафик сначала проверяется на соответствие inside destination NAT. Если он соответствует — адрес назначения меняется на следующий в пуле и трансляция заносится в список трансляций. После этого пакет с уже измененным адресом назначения подвергается маршрутизации.**

- **Обратная трансляция. inside-to-outside. Здесь сначала отрабатывает маршрутизация, если она бросает трафик с inside на outside и есть соответствующая запись в таблице трансляций — пакет транслируется.**

Конфигурирование Inside Destination NAT

Конфигурирование Inside Destination NAT

Сначала создаем пул. Адреса в пуле — адреса наших серверов

```
ip nat pool NAME_OF_POOL 10.0.0.1 10.0.0.10 netmask 255.255.255.0
type rotary
```

слово rotary — для этого типа NAT пул должен быть ротационным (т.е. мы как раз указываем, что адреса будут браться один за другим по кругу, иначе по достижению конца пула следующий пакет будет убит).

Создаем access-list, который будет выделять трафик, подлежащий трансляции. Специально делаем его расширенным:

```
access-list 100 permit  tcp any host 11.1.1.1 eq www
```

Т.е. транслировать будем трафик, направленный к нашему глобальному адресу и даже конкретному порту (TCP!).

Создаем трансляцию:

```
ip nat inside destination list 100 pool NAME_OF_POOL
```

Конфигурирование Inside Destination NAT

Конфигурирование Inside Destination NAT

Маркируем интерфейсы (там где сервера — inside, где внешний мир — outside)

int fa0/0 ip nat insideint fa0/1 ip nat outside

И теперь, можем пронаблюдать картину обращений к нашему серверу:

R3#sh ip nat translations

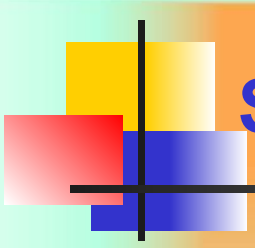
Pro	Inside global	Inside local	Outside local	Outside global
tcp	11.1.1.1:80	10.0.0.1:80	11.1.1.251:18747	11.1.1.251:18747
tcp	11.1.1.1:80	10.0.0.2:80	11.1.1.250:52943	11.1.1.250:52943

Видно, что один и тот же порт глобального адреса (а именно 11.1.1.1:80) транслировался в разные адреса.

Типы реализации NAT overload

Существует 4 типа реализации NAT overload :

- **Symmetric NAT;**
- **Full Cone NAT;**
- **Address Restricted Cone NAT ;**
- **Port Restricted Cone NAT .**



Symmetric NAT

До недавнего времени это была наиболее распространённая реализация. Его характерная особенность - в таблице NAT маппинг адреса IL на адрес IG жёстко привязан к адресу OG, то есть к адресу назначения, который был указан в исходящем пакете, инициировавшем этот маппинг.

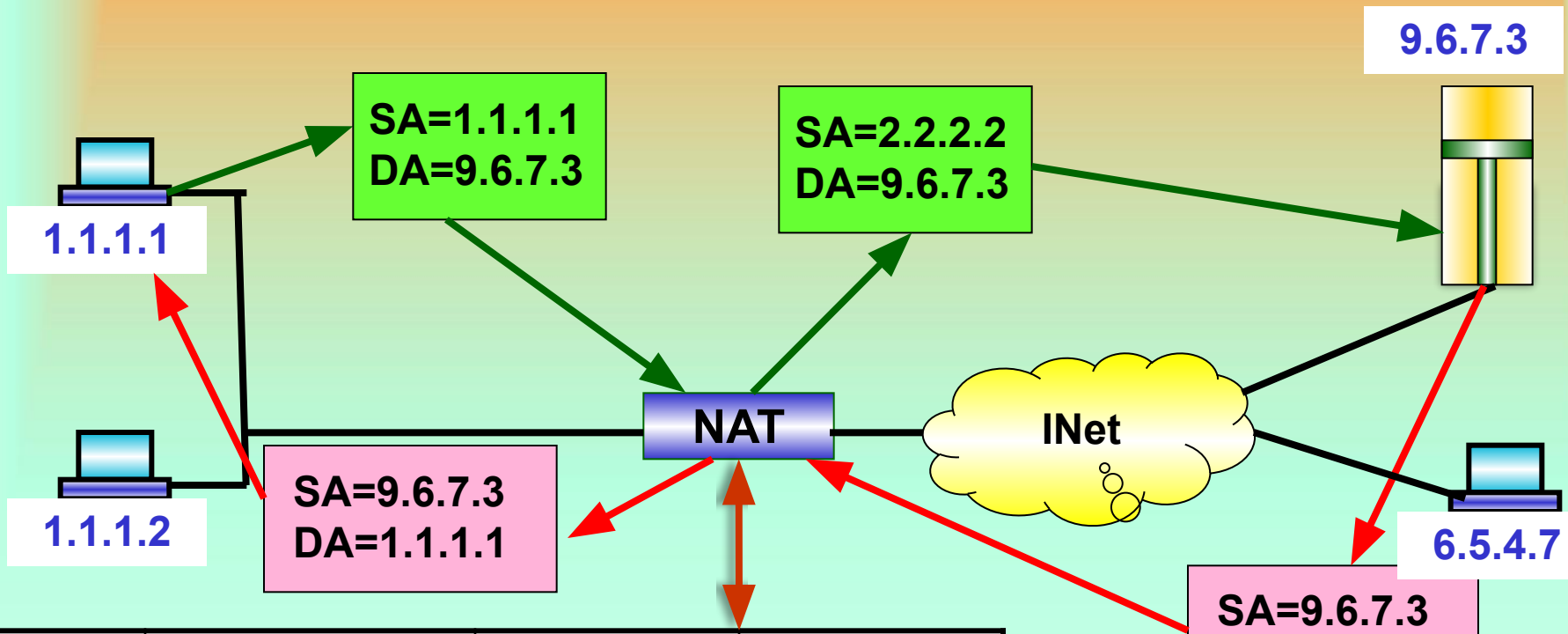
При указанной реализации NAT в нашем примере хост 1.1.1.1 получит оттранслированные входящие UDP-пакеты только от хоста 9.6.7.3 и строго с портом источника 23 и портом назначения 1024 - ни от кого более.

Symmetric NAT

Пакеты от других хостов, даже если указанные в пакете адрес назначения и порт назначения присутствуют в таблице NAT, будут уничтожаться маршрутизатором. Это наиболее параноидальная реализация NAT, обеспечивающая более высокую безопасность для хостов локальной сети.

Корпоративные сети. Маскарадинг.

N внутренних локальных IP ⟺ **1 внешний глобальный IP**



Протокол	Внутр. Локальный адрес	Внутр. Глобальный адрес	Внешний Глобальный адрес
TCP	1.1.1.1 :1024	2.2.2.2 : 1024	9.6.7.3 : 23
TCP	1.1.1.1: 1024	2.2.2.2 : 1024	6.5.4.7 : 80

Extended Entry

Full Cone NAT

Эта реализация NAT - полная противоположность предыдущей. При Full Cone NAT входящие пакеты от любого внешнего хоста будут оттранслированы и переправлены соответствующему хосту в локальной сети, если в таблице NAT присутствует соответствующая запись. Более того, номер порта источника в этом случае тоже не имеет значения - он может быть и 23, и 80, и вообще каким угодно.

Full Cone NAT

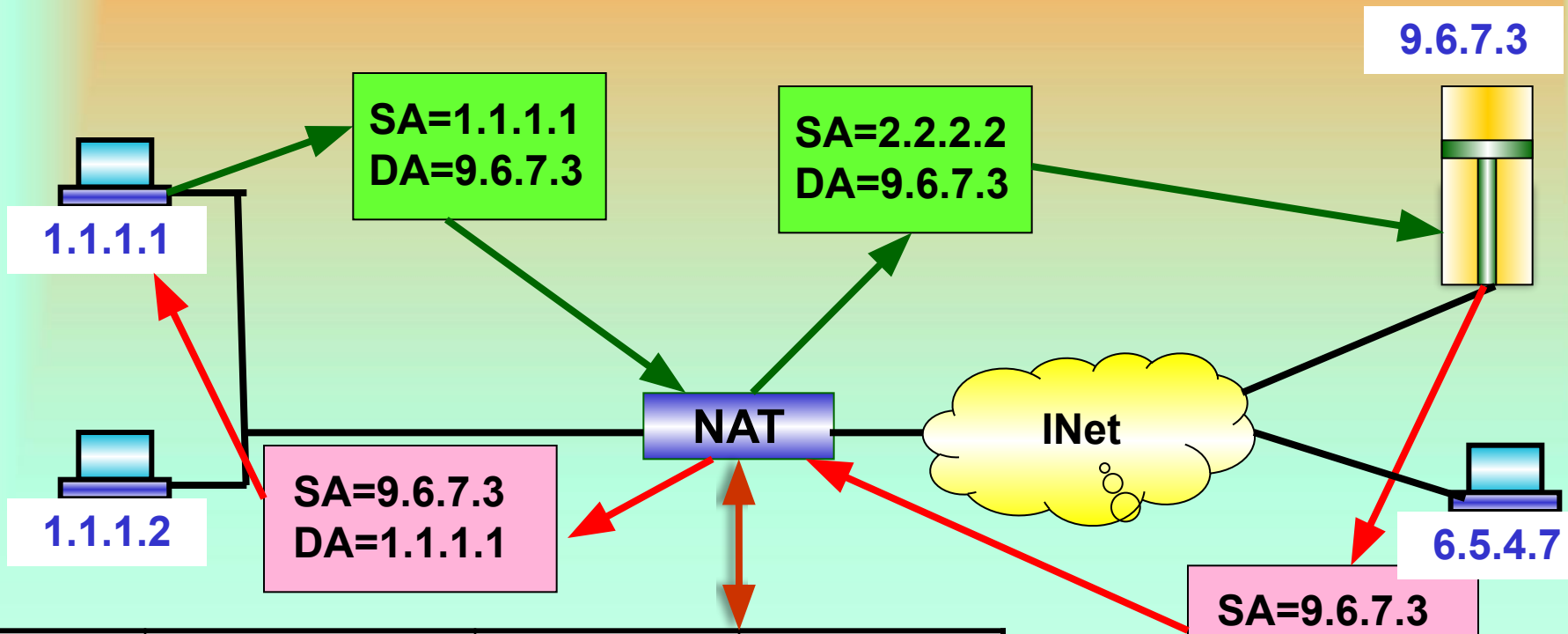
Например, если некое приложение, запущенное на компьютере в локальной сети, инициировало получение пакетов UDP от внешнего хоста 9.6.7.3 на локальный порт 1024, то пакеты UDP для этого приложения смогут слать также и 6.5.4.7, и вообще все до тех пор, пока запись в таблице NAT не будет по какой-либо причине удалена.
Ещё раз: в этой реализации NAT во входящих пакетах проверяется только транспортный протокол, адрес назначения и порт назначения, адрес и порт источника значения не имеют.

Address Restricted Cone NAT

Address Restricted Cone NAT (он же Restricted NAT). Эта реализация занимает промежуточное положение между Symmetric и Full Cone реализациями NAT - маршрутизатор будет транслировать входящие пакеты только с определенного адреса источника (в нашем случае 9.6.7.3), но номер порта источника при этом может быть любым.

Корпоративные сети. Маскарадинг.

N внутренних локальных IP ⟺ **1 внешний глобальный IP**



Протокол	Внутр. Локальный адрес	Внутр. Глобальный адрес	Внешний Глобальный адрес
TCP	1.1.1.1 :1024	2.2.2.2 : 1024	9.6.7.3 : 23
TCP	1.1.1.1: 1024	2.2.2.2 : 1024	9.6.7.3 : 80

Extended Entry

Port Restricted Cone NAT

Port Restricted Cone NAT (или Port Restricted NAT). То же, что и Address Restricted Cone NAT, но в этом случае 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 обязан быть 23, в противном случае пакет будет уничтожен маршрутизатором.

Достоинства и недостатки

Достоинства:

- **Решает проблему нехватки IP-адресов;**
- **Скрывает от посторонних глаз структуру корпоративной сети;**
- **Выполняет функции файрвола**

Достоинства и недостатки

Недостатки:

- **Принцип NAT не вписывается в архитектуру IP, которая предполагает, что каждый IP-адрес уникальным образом идентифицирует только одну машину в мире. При использовании NAT, тысячи машин могут иметь адрес 10.0.0.1.**
- **NAT нарушает «сквозной» принцип, согласно которому каждый хост должен иметь возможность отправлять пакет другому хосту в любой момент времени. На самом деле, входящие пакеты не принимаются до тех пор, пока не отправятся исходящие. Т.е.удаленный пользователь не может подключиться к корпоративной сети.**

Достоинства и недостатки

- NAT превращает интернет из сети без установления соединений в подобие сети ориентированной на соединения. NAT-блок поддерживает таблицу отображающую все соединения компьютеров корпоративной сети с интернетом. Если NAT ломается все TCP соединения теряются безвозвратно. При отсутствии NAT, выход из строя (перезагрузка) маршрутизатора вызывает лишь небольшую задержку – отправляющий процесс посылает заново все неподтвержденные пакеты. Т.е. IP сеть становится восприимчивой к сбоям как и сеть с коммутацией каналов.

Достоинства и недостатки

- NAT нарушает фундаментальное правило построения многоуровневых протоколов: уровень k не должен использовать информацию уровня k+1. Если на смену TCP придет TCP-2 с другим форматом, то NAT не будет работать. Идея многоуровневых протоколов состоит в том, чтобы изменения на одном уровне не могли повлиять на остальные уровни. NAT разрушает эту независимость.
- Существуют приложения (FTP, IP-телефония и др.), которые могут отказаться работать с NAT без принятия специальных мер.