*Защита №3*

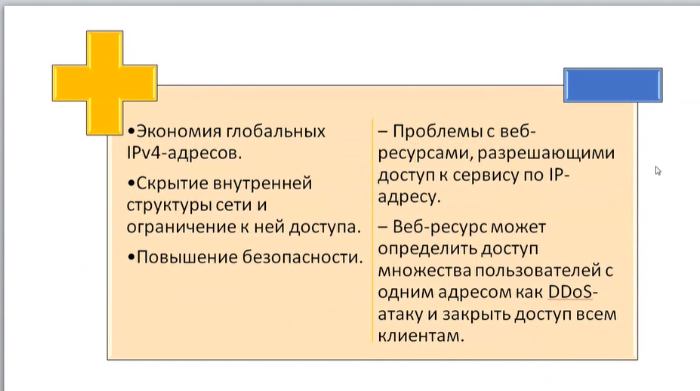
ТРАНСЛЯЦИЯ СЕТЕВЫХ АДРЕСОВ

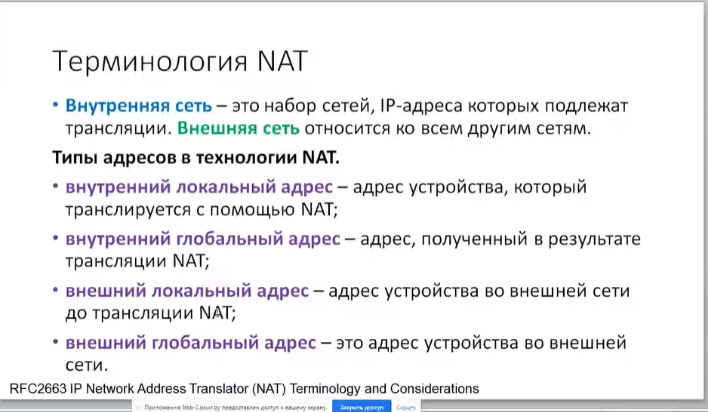
1. **Определение и назначение технологии NAT. Типы адресов в NAT.**

NAT (Network Address Translation) - трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах. NAT используется чаще всего для осуществления доступа устройств из корпоративной (частной) cети в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети. Для преобразования частных адресов в глобальные (маршрутизируемые в Интернете) применяют NAT.

Помимо возможности доступа в глобальную сеть Интернет, NAT имеет ещё несколько положительных сторон. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. Также эта технология позволяет экономить глобальные IРv4-адреса, так как под одним глобальным адресом в Интернет может выходить множество устройств.

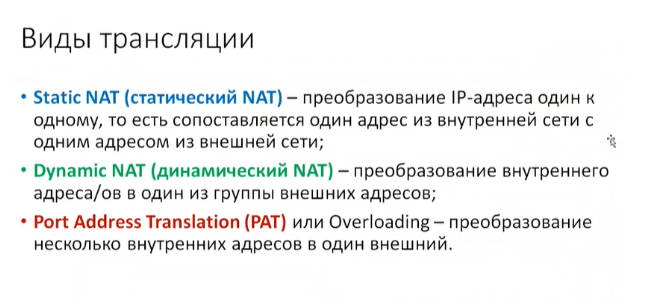
Технология NAT обеспечивает преобразование частных адресов в публичные. Это позволяет устройству с частным IPv4-адресом получать доступ к ресурсам за пределами корпоративной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных адресов IPv4. Один общедоступный IPv4-адрес может использоваться сотнями и тысячами устройствами, каждое из которых имеет уникальный частный IPv4-адресс.







1. **Различия в видах трансляции IP-адресов.**



При *статическом NAT* после отправки сообщения с устройства внутренней сети маршрутизатор преобразует внутренний локальный адрес во внутренний глобальный адрес. Статический NAT особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из глобальной сети. Также статический NAT может применяться для устройств, которые должны быть доступны для авторизованного персонала вне сети, например, доступ по SSH к настройкам сетевого оборудования. Основное требование при

использование статического NAT - доступность достаточного количества адресов.

*Динамический NAT* использует пул публичных адресов и назначает их в порядке очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT назначает доступный общедоступный IРv4-адрес из пула.

*РАТ* иногда называется Overloading сопоставляет несколько частных адресов IPv4 с одним общедоступным адресом IPv4. В большинстве случаев домашние маршрутизаторы используют именно эту технологии трансляции IPv4-адресов. Интернет-провайдер назначает маршрутизатору один адрес, но несколько устройств, подключенных к одному домашнему маршрутизатору, могут одновременно иметь доступ к Интернету.

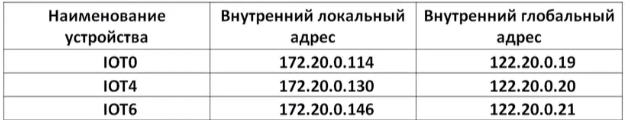
1. **Последовательность действий и пример конфигурации статического NAT. Способы проверки конфигурации NAT**

Для конфигурации статического NAT необходимо выполнить следующие

действия:

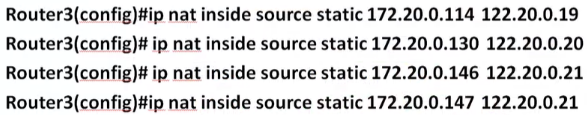
1. спланировать сопоставление внутренних локальных 1Ру4-адресов и

внутренних глобальных;



2) осуществить конфигурацию статического NAT с помощью команды

ip nat inside source static Внутренний\_локальный\_адрес Внуренний\_глобальный\_адрес;



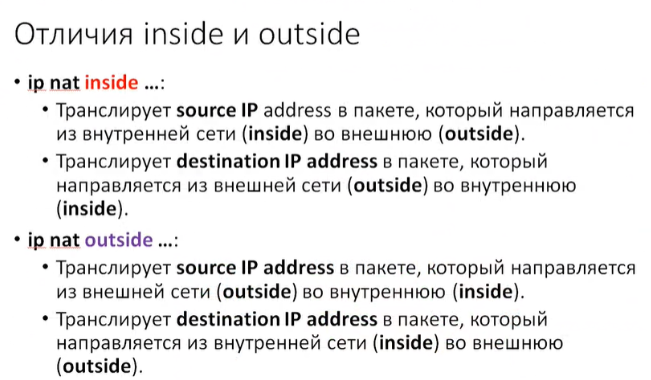
3) определить какие интерфейсы маршрутизатора относятся к внутренней

сети; осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды *ip nat inside*; определить какие интерфейсы маршрутизатора относятся к внешней сети;осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды

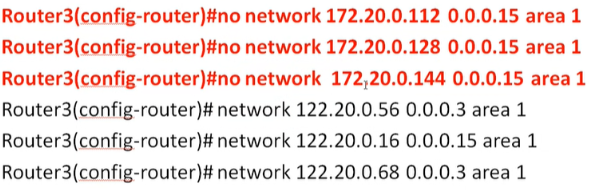
*ip nat outside*.



Дополнение:



4)изменение конфигурации маршрутизатора



Проверка конфигурации NAT:

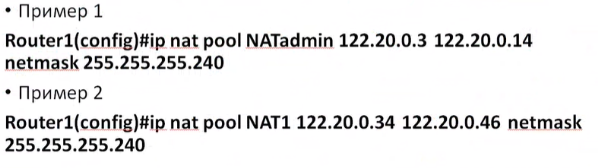
* show ip nat translations
* show ip nat statistics

1. **Последовательность действий и пример конфигурации динамического NAT**

Для конфигурации динамического NAT необходимо выполнить следующие действия.

1.Определить пул адресов, которые будут использоваться для трансляции, помощью команды

*ip nat pool имя\_пула начальный\_1Р-адрес конечный\_1Р-адрес netmask маска\_подсети.*



2. Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды

*access-list номерАСL permit IPадреc внутренней\_сети обратная\_маска\_внутренней\_сети*

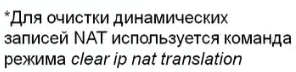
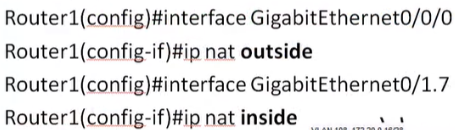
**

3. Установить связь созданного ACL с пулом с помощью команды

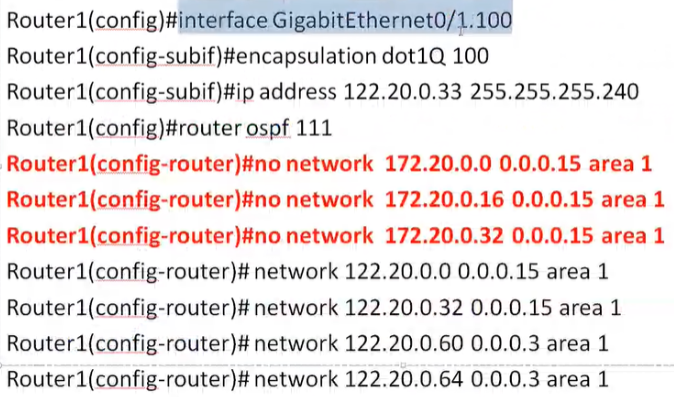
*ip nat inside source list номер\_АСL pool имя\_пула*. Эта конфигурация используется маршрутизатором для определения того, какие устройства (номер АСL) получают, какие адреса (имя пула).



4. Определить какие интерфейсы маршрутизатора относятся к внутренней сети, на интерфейсах с указанием их подключения к внутренней сети с помощью *ip nat inside*. И какие относятся к внешней сети с помощью команды *ip nat outside*.



5, Изменение конфигураци маршрутизации



Проверка конфигурации NAT:

* show ip nat translations
* Sh ip nat statistics

Отключение функции демонстрации процесса преобразования на маршрутизаторе

* Debug ip nat

1. **Последовательность действий и пример конфигурации РАТ для диапазона публичных IP-адресов. = (динамический)**

1. Определить пул глобальных адресов, которые будут использоваться

для трансляции, с помощью команды

*ip nat pool имя\_пула начальный IР-адрес конечный IР-адрес netmask маска\_подсети.*



2. Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды *access-list номерАСL permit IPадрес внутренней сети обратная маска внутренней сети.*



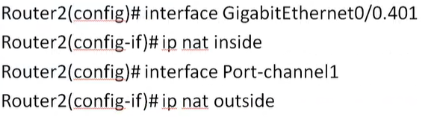
3. Установить связь созданного ACL с пулом и типом NAT с помощью команды

*ip nat inside source list номер\_АСЬ pool имя\_пула overload.*

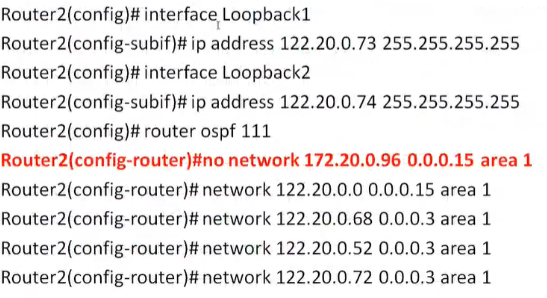
**

4. Определить какие интерфейсы маршрутизатора относятся к внутренней сети –

ip nat inside. к внешней сети с помощью команды ip nat outside



5, Изменение конфигурации маршрутизации



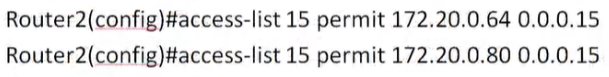
Проверка конфигурации PAT

* Show ip nat translations
* Show ip nat stat

1. **Последовательность действий и пример конфигурации РАТ для одного публичного IP-адреса.**

1, Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды

*access-list номерАСL permit IPадрес\_внутренней\_сетобратная\_маска\_внутренней\_сети.*



2. Конфигурация РАТ с указанием номера списка контроля доступа и типа и номера интерфейса, IP-адрес которого будет использован для трансляции, с помозью команды *ip nat inside source list номер\_АСЬ interface тип\_номер overload.*



3. Определить какие интерфейс к внутренней сети и к внутренней сети с помощью команды ip nat inside. И ip nat outside

