Б-Безопасность

ACL, NAT, VPN

Задача: Соединить два удаленных офиса

- Физический канал
  - Ethernet – витая пара
  - WiFi
  - xDSL
  - Радио-Релейные Линии
  - Оптоволокно

Задача: Соединить два удаленных офиса

- Аренда канала у провайдера
  - Прямой кабель
  - L2VPN
  - L3VPN

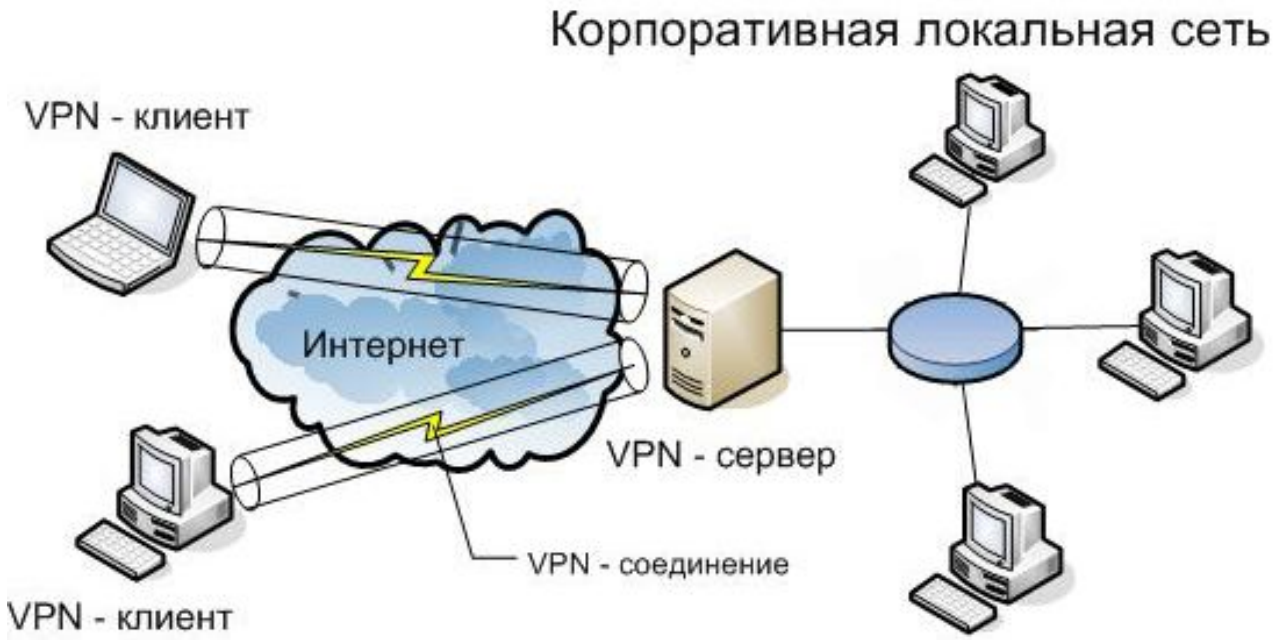
Задача: Соединить два удаленных офиса

- Туннель через публичную сеть
  - GRE
  - IPSec
  - GRE over IPSec
  - VTI
  - DMVN

VPN

- VPN - *Virtual Private Network* - виртуальная частная сеть
  - Технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети.

VPN


Корпоративная локальная сеть
VPN - клиент
Интернет
VPN - сервер
VPN - соединение
VPN - клиент

Преимущества VPN

- Масштабируемость
- Сокращение затрат
- Безопасность

Типы VPN

- Site-to-site
  - Используется для соединения между собой нескольких офисов
- Remote access
  - Используется для подключения удаленных сотрудников

Свойства VPN-подключений

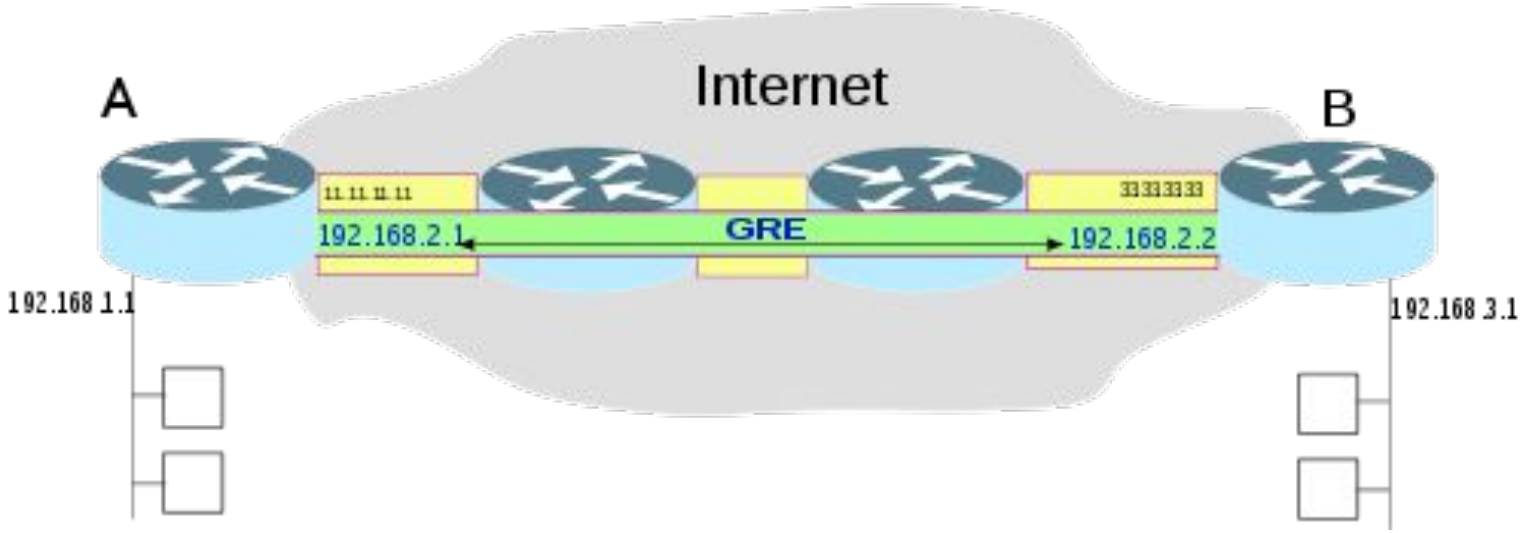
- Инкапсуляция
- Подлинность
- Шифрование данных

Туннелирование

- **Туннелирование**— процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

GRE

- **GRE** – Сетевой протокол от компании *CISCO* для туннелирования соединений, путем инкапсуляции пакетов сетевого уровня в IP пакеты.



GRE

IPSec

- **IPsec** (сокращение от **IP Security**)
  - набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP

Функции IPSec

- Шифрование
- Целостность данных
- Аутентификация
- Защита от повторов

Набор протоколов IPSec

Протокол	RFC	Описание
Authentication Header (AH)	4302	Обеспечивает целостность передаваемых данных, аутентификацию источника информации и replay protection
Encapsulating Security Payload (ESP)	4303	Обеспечивает шифрование, целостность передаваемых данных, аутентификацию источника информации и replay protection
Internet Key Exchange (IKE)	2409, 4109, 4306	Обеспечивает согласование протоколов и безопасный обмен ключами

IPSec

Протокол	RFC	Описание
HMAC: Keyed-Hashing for Message Authentication	2104	Аутентификация
Diffie-Hellman Key Agreement Method	2631	Алгоритм обмена ключами
MD5, SHA	2403, 2404	Проверка целостности

Транспортный режим

- Обеспечивается аутентификация или шифрование поля данных IP-пакета
- Информация сетевого уровня известна (отправитель и адресат)
- Host-to-host взаимодействие

Туннельный режим

- Обеспечивается аутентификация или шифрование всего IP-пакета
- Классический VPN

AH заголовок

Защита от подмены исходного пакета, включая адрес отправителя
AH заголовок располагается после IP – заголовка

ESP

- ESP - протокол, обеспечивает конфиденциальность и защиту данных.

Access control lists

- Являются универсальным селектором трафика
- Могут использоваться в том числе и для ограничения доступа

Виды ACL

- По типу фильтрации
  - Standard
    - Могут фильтровать только по условию исходящего IP
  - Extended
    - Могут фильтровать по IP адресам и портам источника и назначения

Виды ACL

- По именованию
  - Нумерованные
    - В качестве идентификатора используют номер
    - Каждая запись задается в режиме глобальной конфигурации
  - Именованные
    - В качестве идентификатора используется имя
    - Каждая запись задается внутри ACL

Примеры

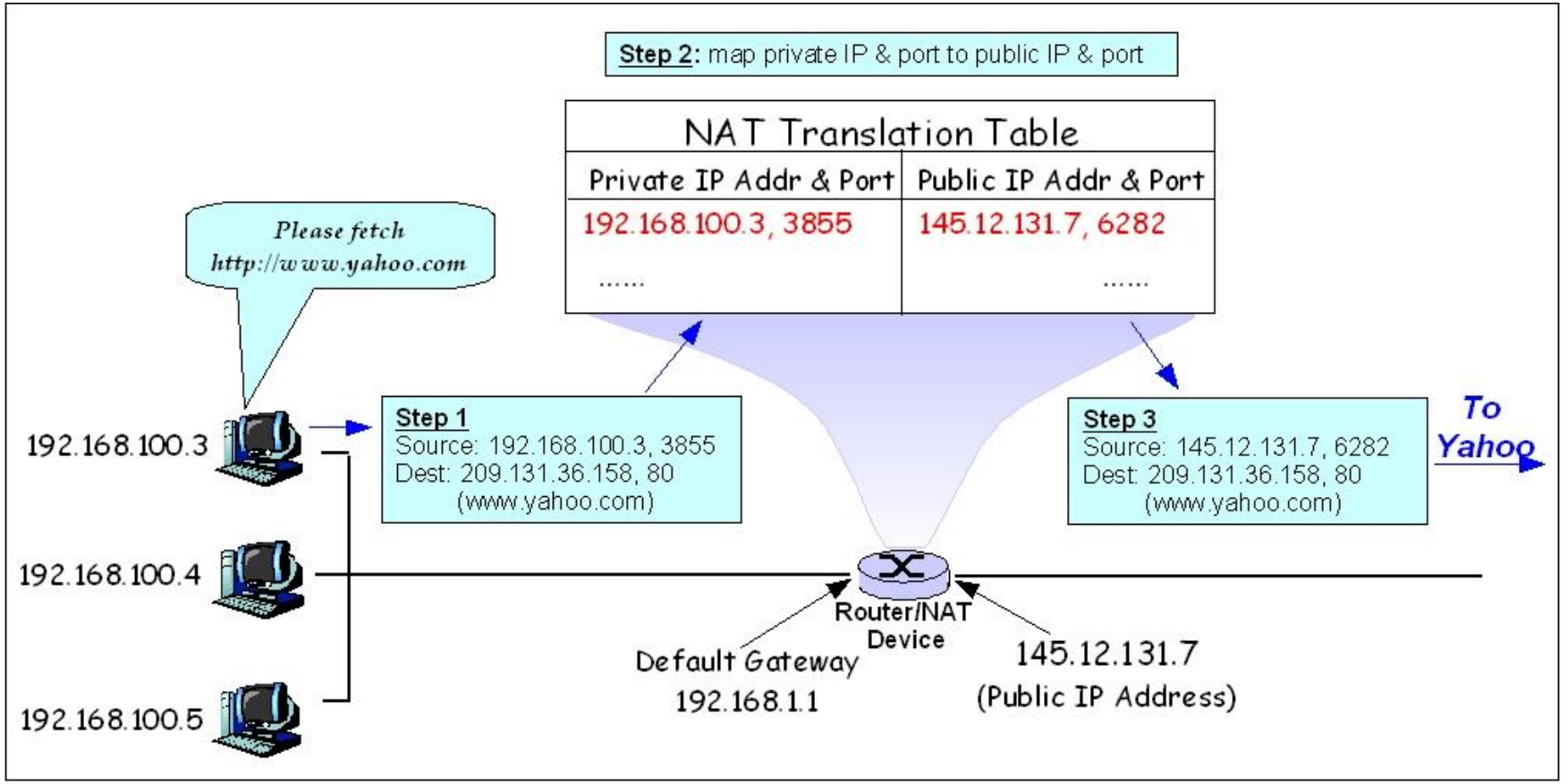
- Расширенный именованный ACL

```
Router(config)#ip access-list extended ACLNAME
Router(config-ext-nacl)#permit udp 192.168.0.0 0.0.0.255 host 8.8.8.8 eq domain
Router(config-ext-nacl)#deny ip any any
```

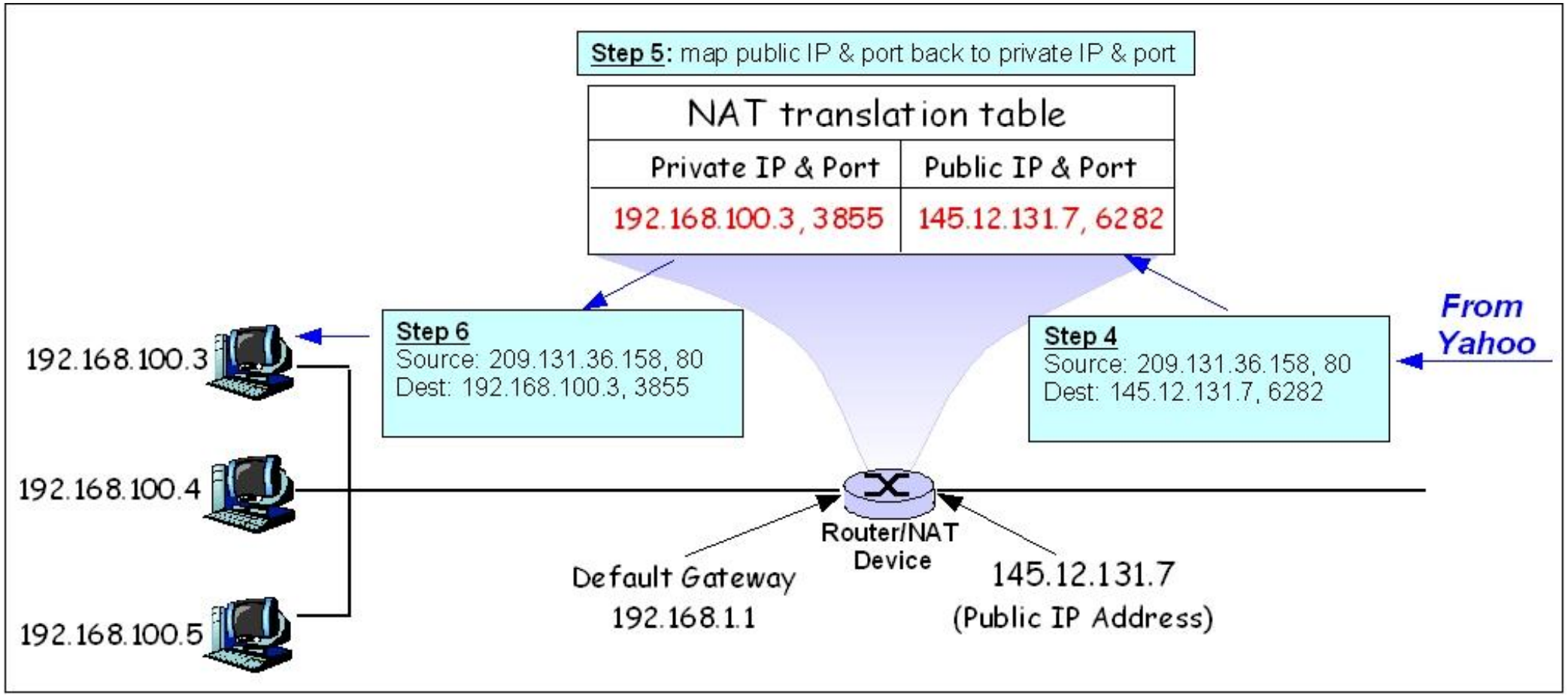
- Стандартный нумерованный ACL

```
Router(config)#access-list 1 permit 192.168.1.1 255.255.255.255
Router(config)#access-list 1 permit 192.168.1.2 255.255.255.255
Router(config)#access-list 1 deny 192.168.1.0 255.255.255.255
```

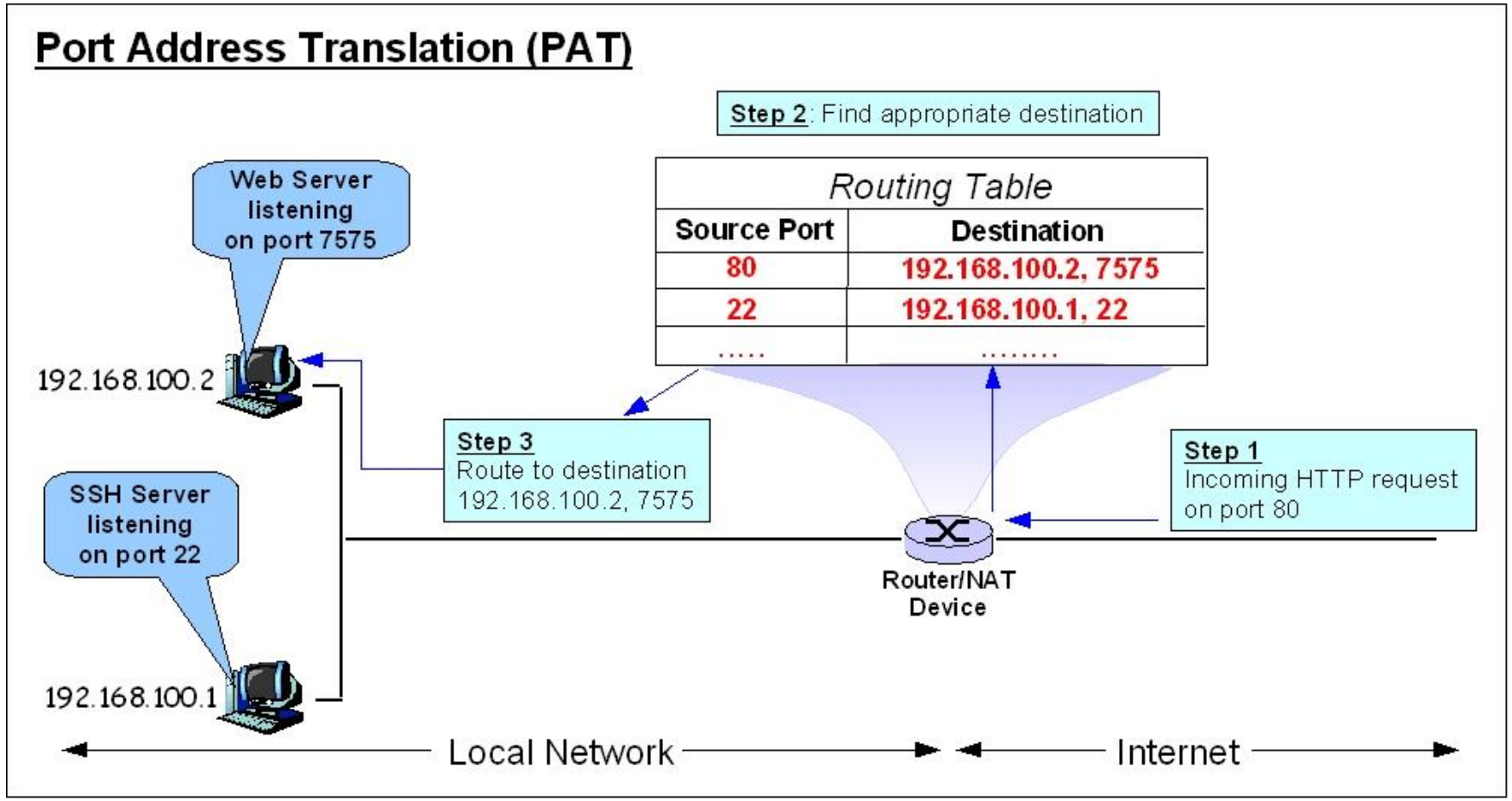
NAT


Step 2: map private IP & port to public IP & port
NAT Translation Table
Private IP Addr & Port
Public IP Addr & Port
192.168.100.3, 3855
145.12.131.7, 6282
.....
.....
Please fetch
http://www.yahoo.com
192.168.100.3
192.168.100.4
192.168.100.5
Step 1
Source: 192.168.100.3, 3855
Dest: 209.131.36.158, 80
(www.yahoo.com)
Step 3
Source: 145.12.131.7, 6282
Dest: 209.131.36.158, 80
(www.yahoo.com)
To Yahoo
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(Public IP Address)

NAT


Step 5: map public IP & port back to private IP & port
NAT translation table
Private IP & Port
Public IP & Port
192.168.100.3, 3855
145.12.131.7, 6282
Step 6
Source: 209.131.36.158, 80
Dest: 192.168.100.3, 3855
Step 4
Source: 209.131.36.158, 80
Dest: 145.12.131.7, 6282
From Yahoo
192.168.100.3
192.168.100.4
192.168.100.5
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(Public IP Address)

PAT


Port Address Translation (PAT)
Step 2: Find appropriate destination
Routing Table
Source Port
Destination
80
192.168.100.2, 7575
22
192.168.100.1, 22
.....
.....
Web Server listening on port 7575
192.168.100.2
SSH Server listening on port 22
192.168.100.1
Step 3
Route to destination 192.168.100.2, 7575
Step 1
Incoming HTTP request on port 80
Router/NAT Device
Local Network
Internet

Пример

```
!
interface GigabitEthernet0/0
ip nat inside
speed auto
!
interface GigabitEthernet0/1
ip nat outside
speed auto
!
ip nat inside source static 192.168.1.1 10.0.0.1
!
```