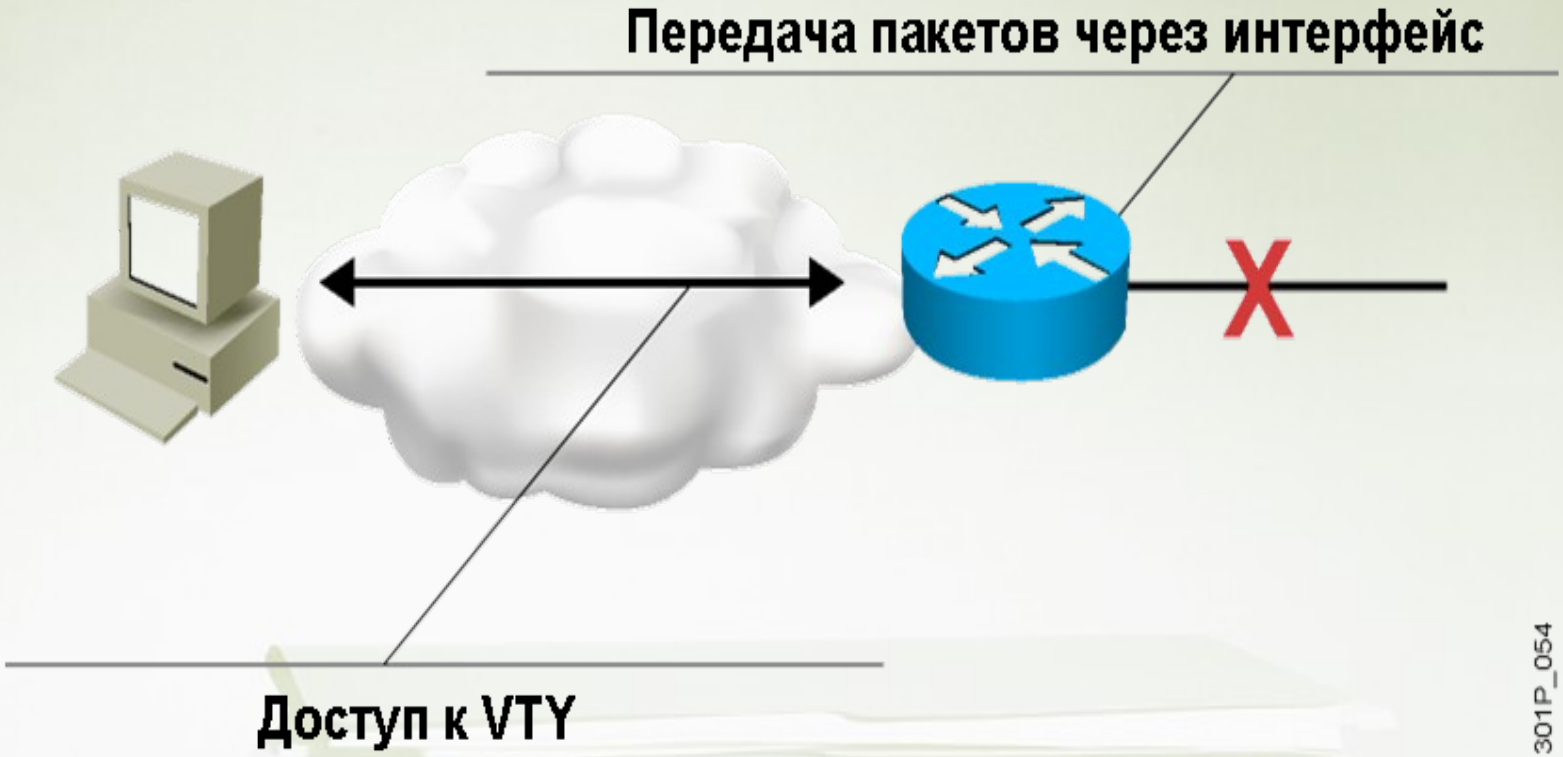
Настройка ACL и NAT

Петухов Андрей
petand@lvk.cs.msu.su
Антоненко Виталий
anvial@lvk.cs.msu.su
комната 247

Для чего нужны ACL?

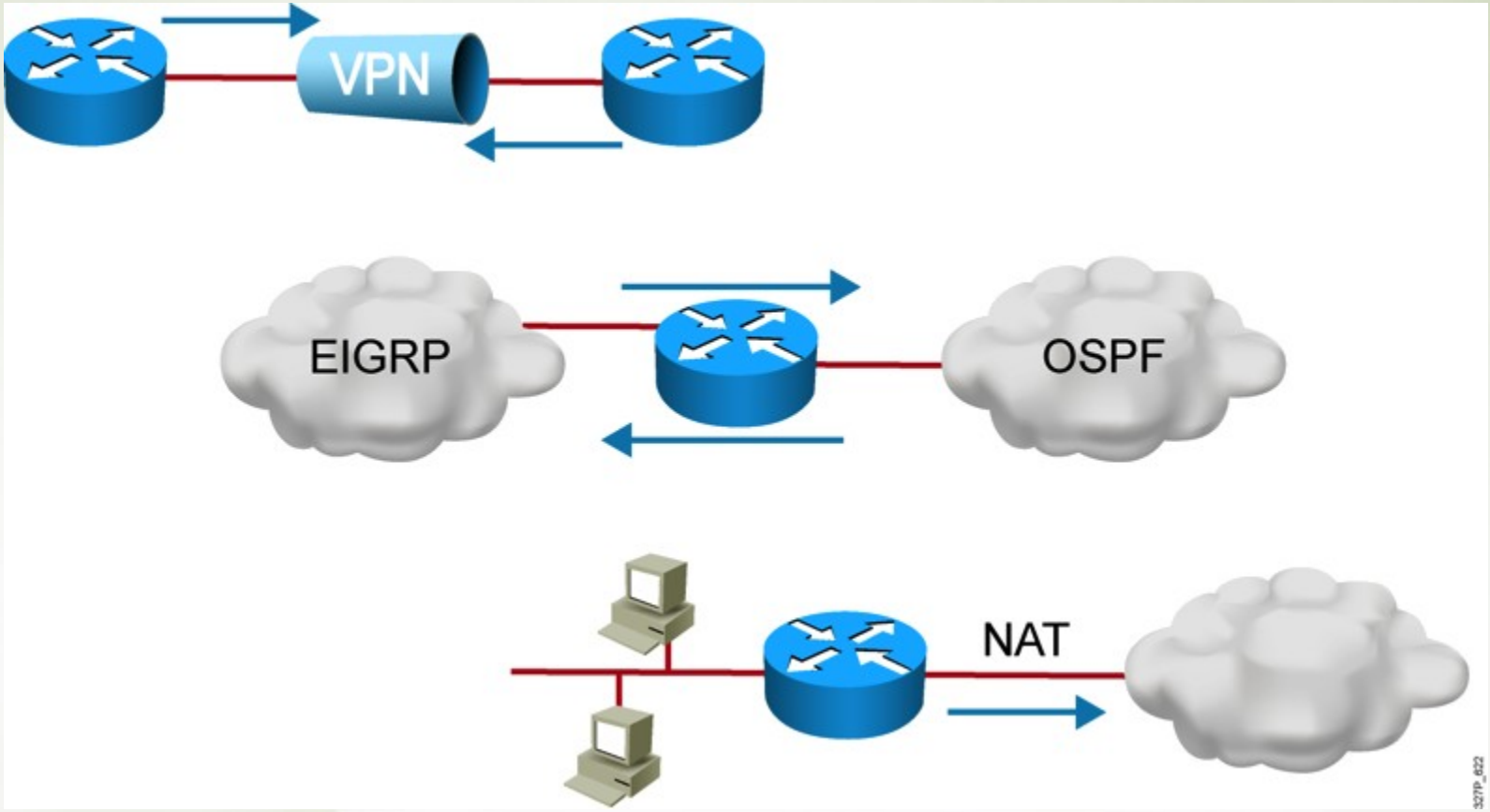
- Классификация: разделение трафика на классы на основе значений полей пакетов
- Фильтрация: один из вариантов использование классов трафика

Фильтрация с помощью ACL

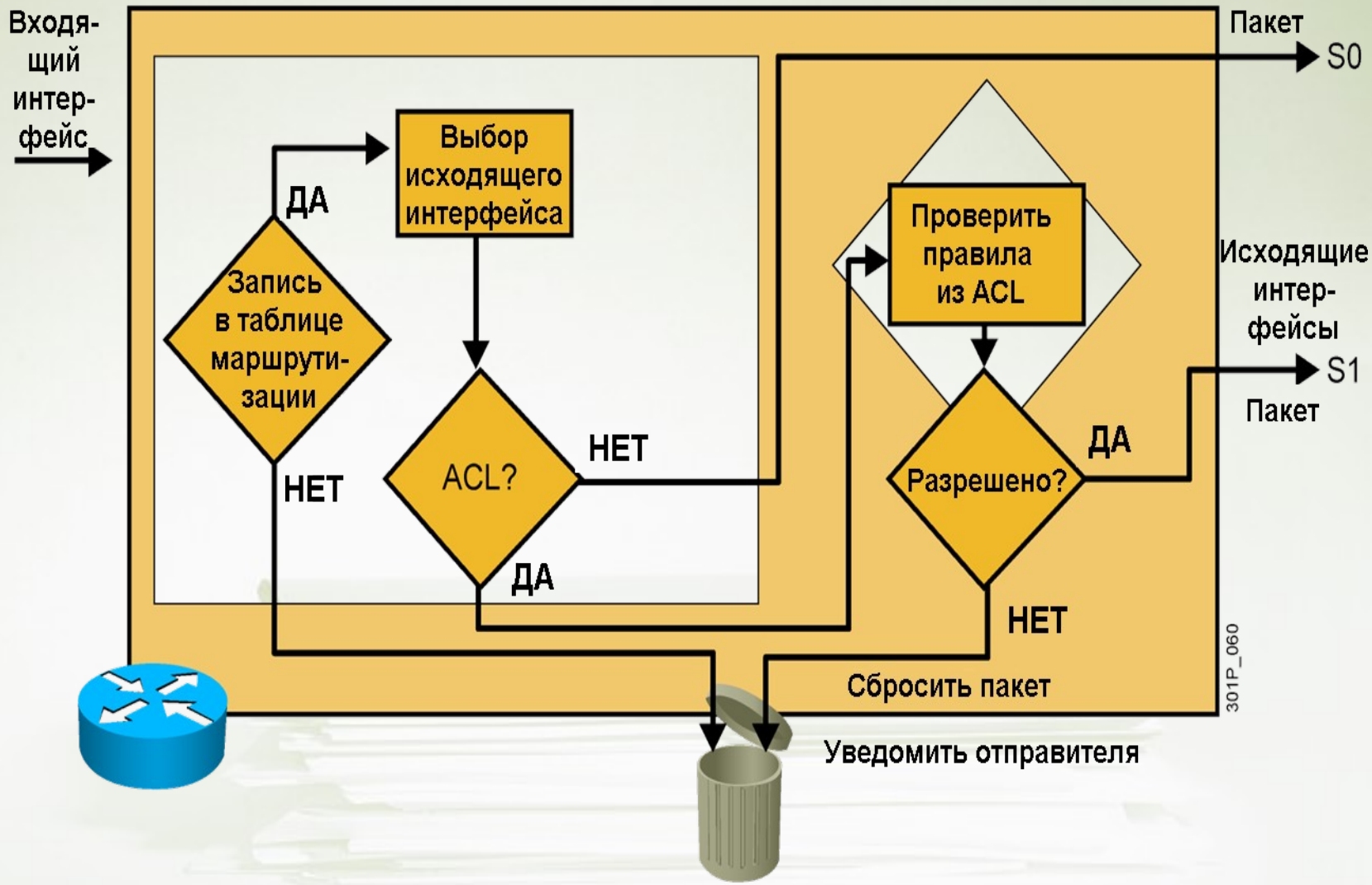


- Можно задать классы разрешенного и запрещенного трафика, проходящего **через** маршрутизатор.
- Можно задать классы разрешенного и запрещенного трафика, предназначенного **самому** маршрутизатору (vty)

Другие применения ACL



ACL в исходящем направлении



Если ни одно правило ACL не сработало, пакет сбрасывается.

Типы ACL (вариант Huawei)

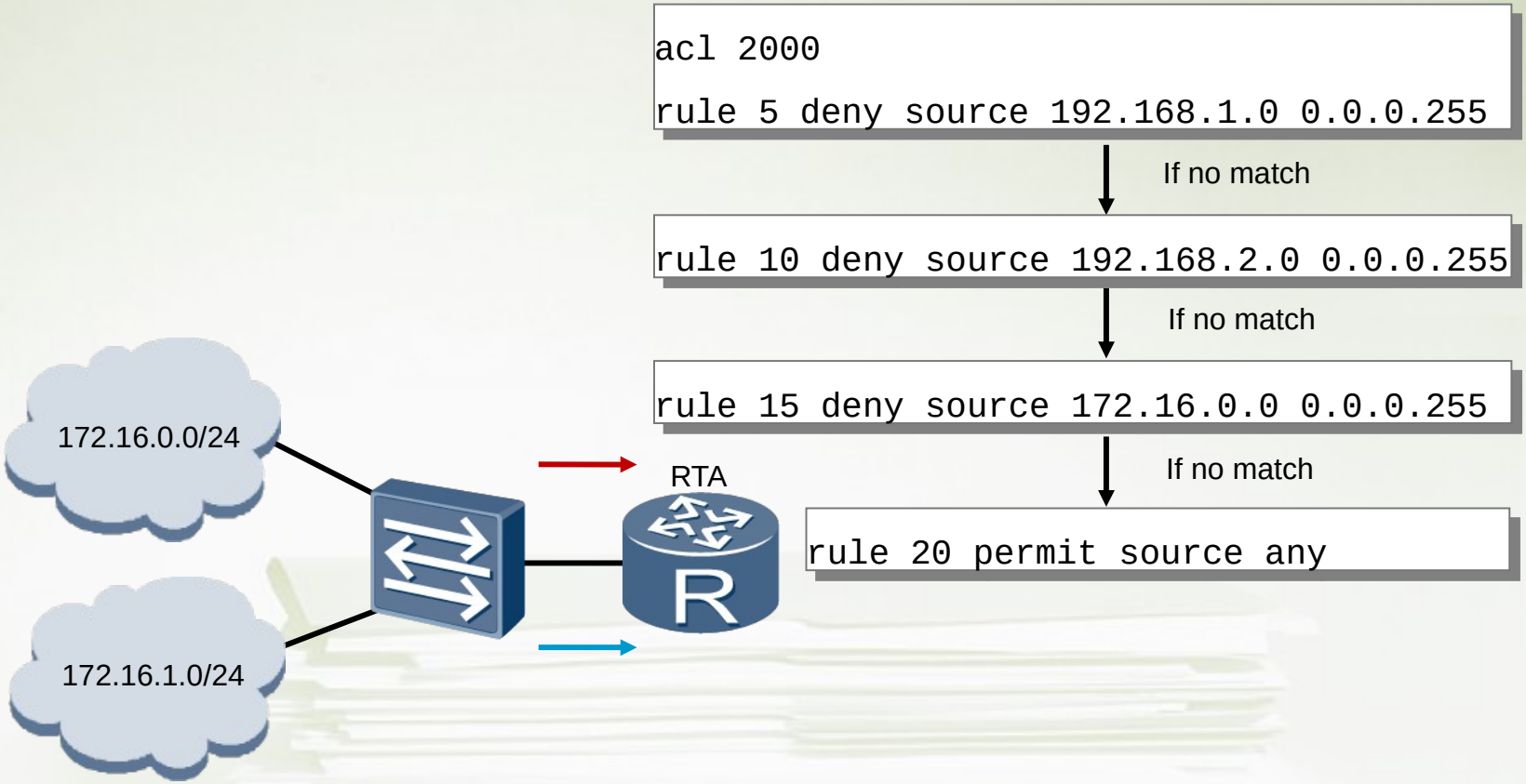
Types	Value Ranges	Parameters
Basic	2000-2999	Source IP
Advanced	3000-3999	Source & Destination IP, Protocol, Source & Destination Port
Layer 2 ACL	4000-4999	MAC Address

Тип ACL (вариант CISCO)

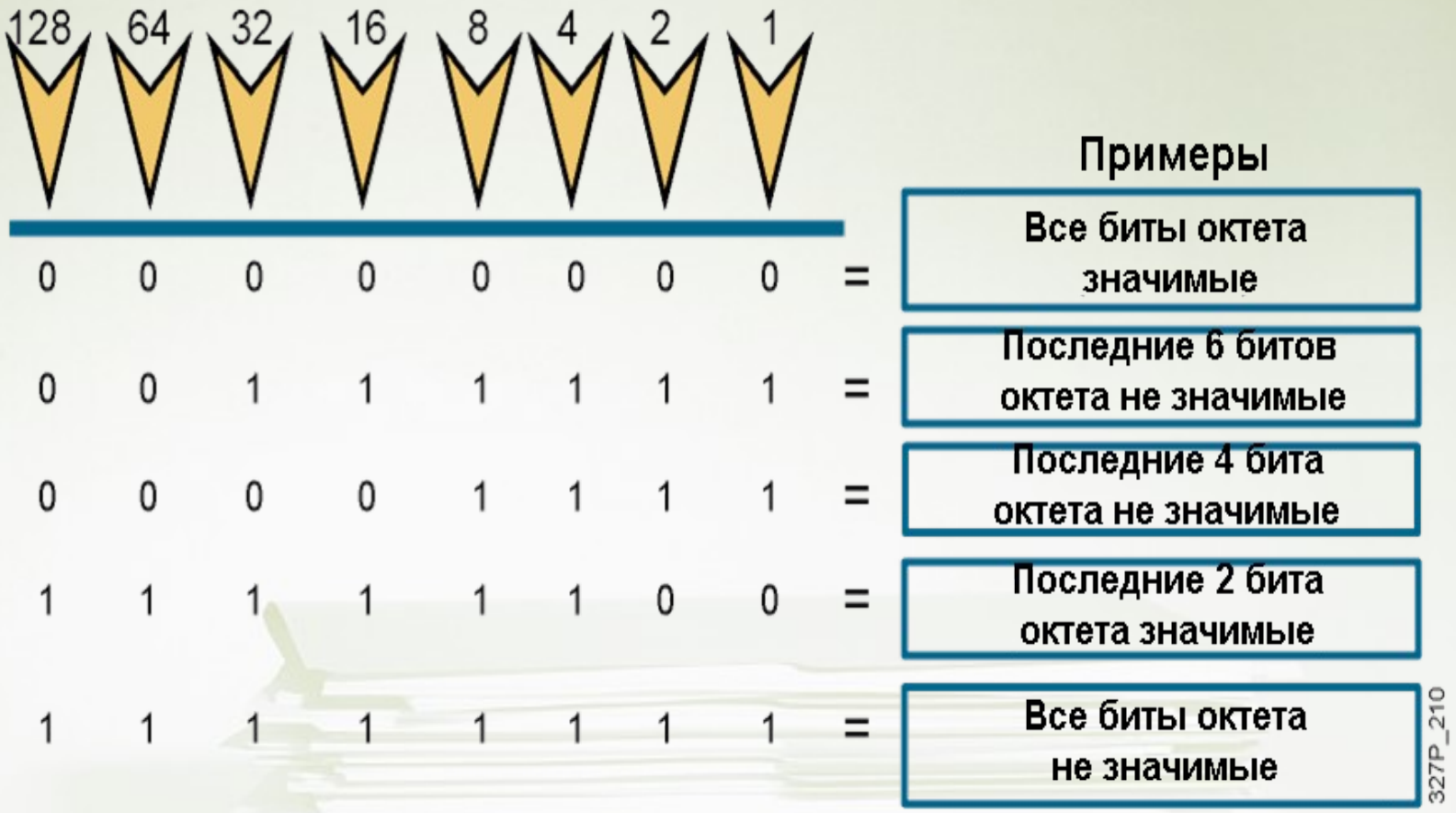
Тип ACL	Тип/Диапазон идентификатора
Нумерованный стандартный	1–99, 1300–1999
Нумерованный расширенный	100–199, 2000–2699
Именованный (стандартный и расширенный)	**Имя**

- Тип нумерованного ACL определяется неявно через присваиваемый ему идентификатор:
  - Использование идентификаторов из диапазона [1–99] и [1300–1999] приведет к созданию стандартного ACL.
  - Использование идентификаторов из диапазона [100–199] и [2000–2699] приведет к созданию расширенного ACL.
- При создании именованного ACL его тип задается явно

Правила ACL


acl 2000
rule 5 deny source 192.168.1.0 0.0.0.255
If no match
rule 10 deny source 192.168.2.0 0.0.0.255
If no match
rule 15 deny source 172.16.0.0 0.0.0.255
If no match
rule 20 permit source any
172.16.0.0/24
172.16.1.0/24
RTA
R

Маски для задания правил ACL



- 0 означает значимый бит в позиции IP адреса
- 1 означает незначимый бит в позиции IP адреса

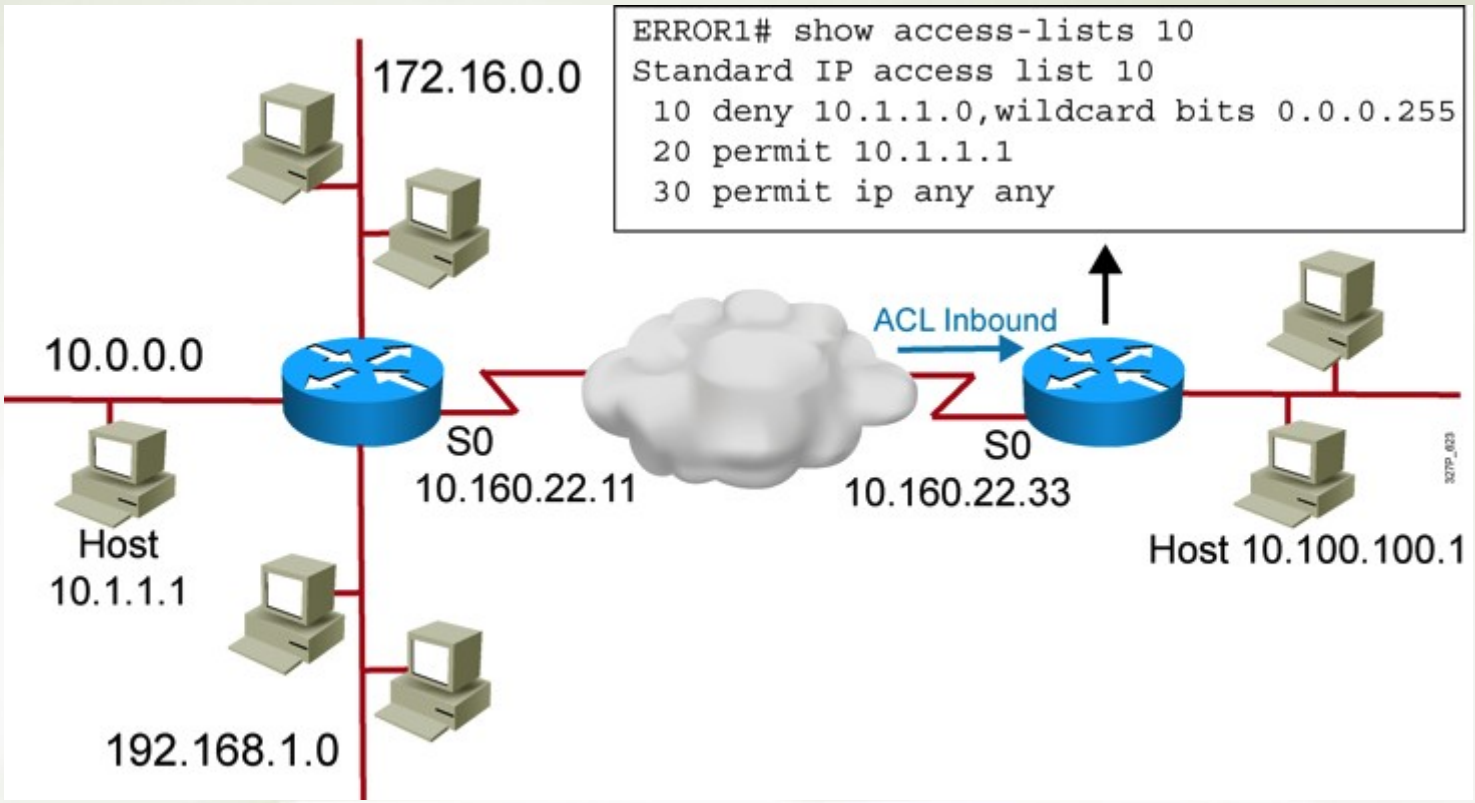
Маски для задания правил ACL, пример

Маска для диапазона адресов 172.30.16.0/24 - 172.30.31.0/24.

маска будет следующей

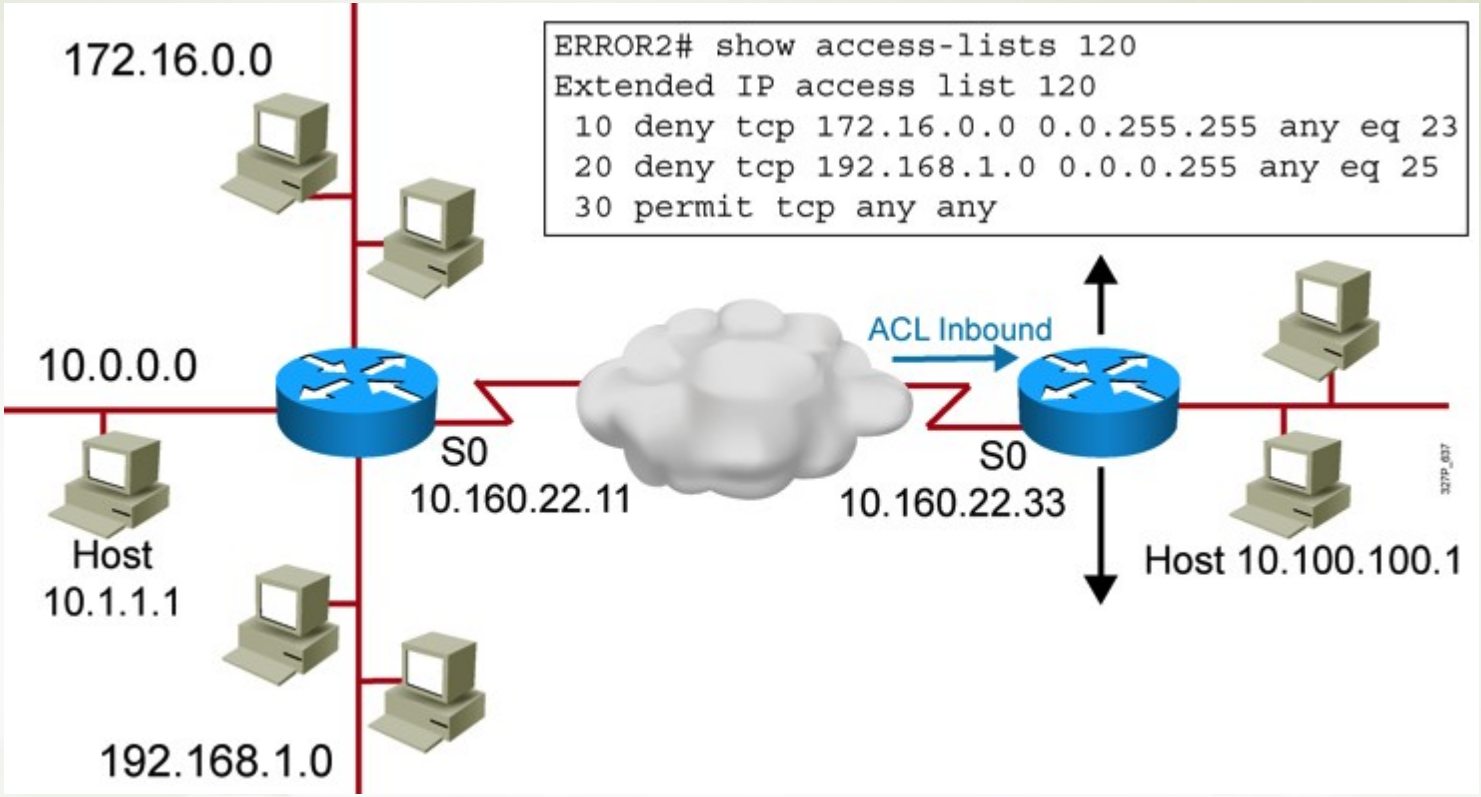
172.30.16.0 0.0.15.255

Типичные ошибки в ACL (1 из 4)



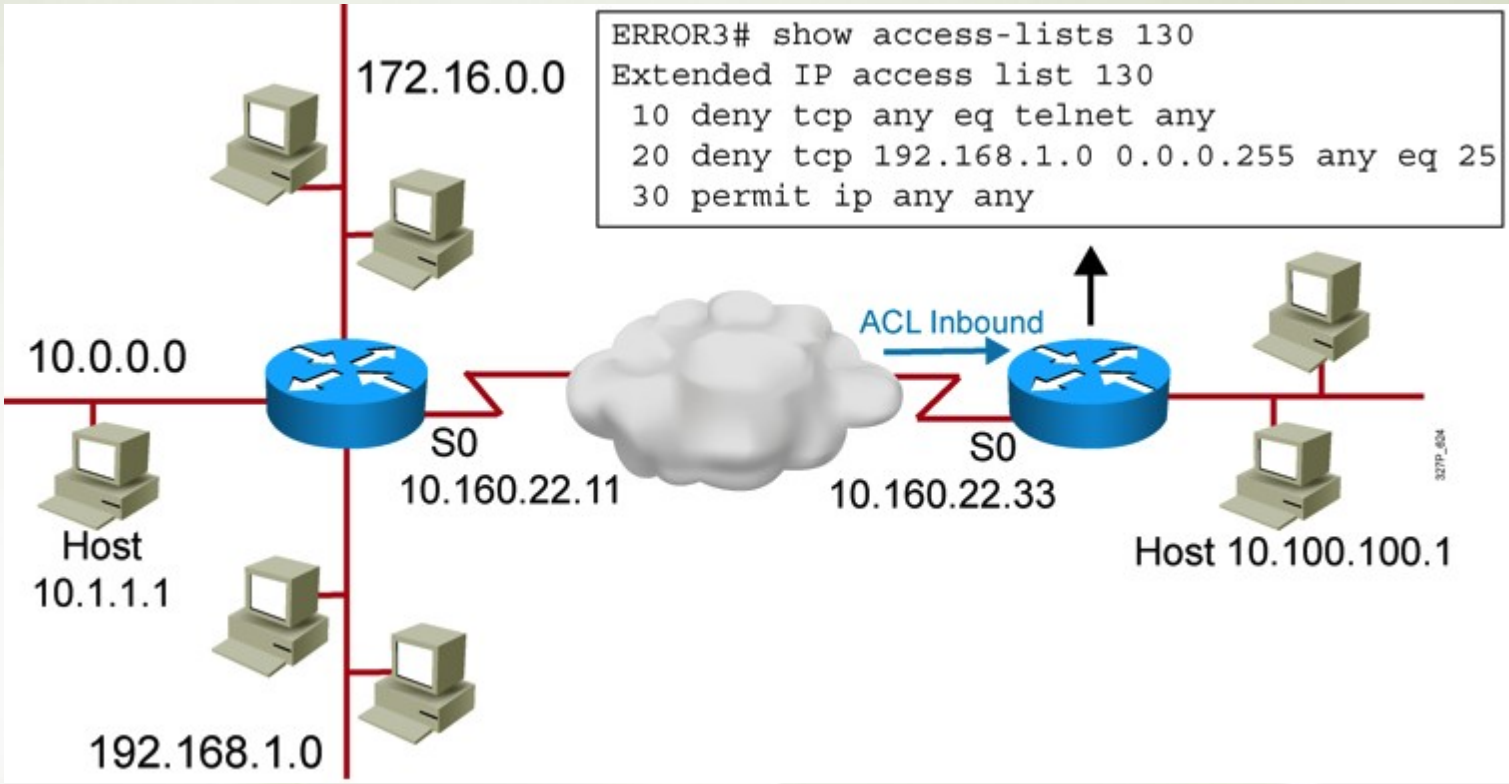
Пример 1: Хост 10.1.1.1 не может подключиться к 10.100.100.1

Типичные ошибки в ACL (2 из 4)



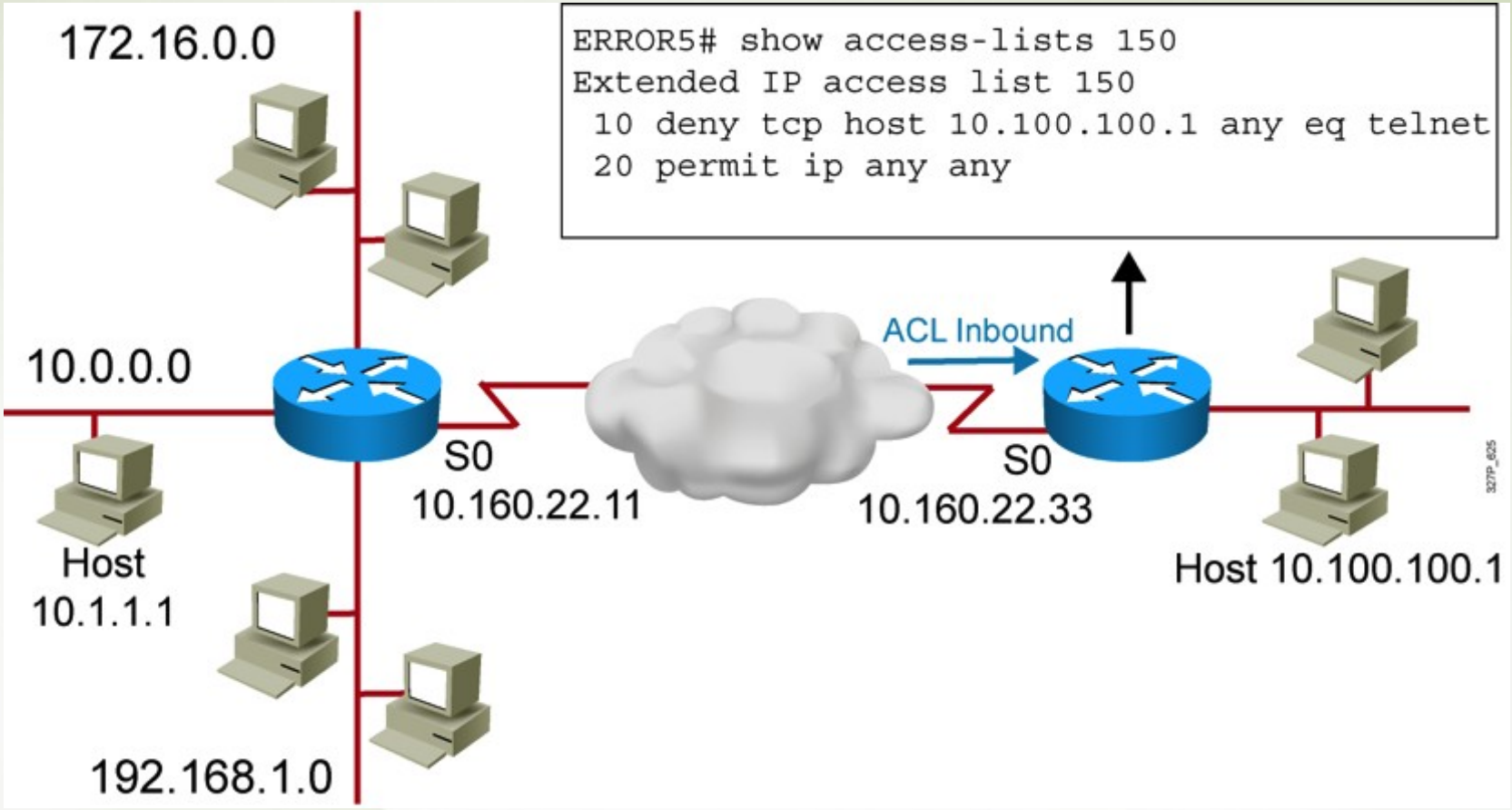
Пример 2: Сеть 192.168.1.0 не может подключиться к 10.100.100.1. по TFTP

Типичные ошибки в ACL (3 из 4)



Пример 3: Сеть 172.16.0.0 может использовать Telnet для подключения к 10.100.100.1, а политикой безопасности это запрещено

Типичные ошибки в ACL (4 из 4)



Пример 4: Хост 10.100.100.1 может использовать Telnet для подключения к 10.1.1.1, а политикой безопасности это запрещено

NAT: Network Address Translation

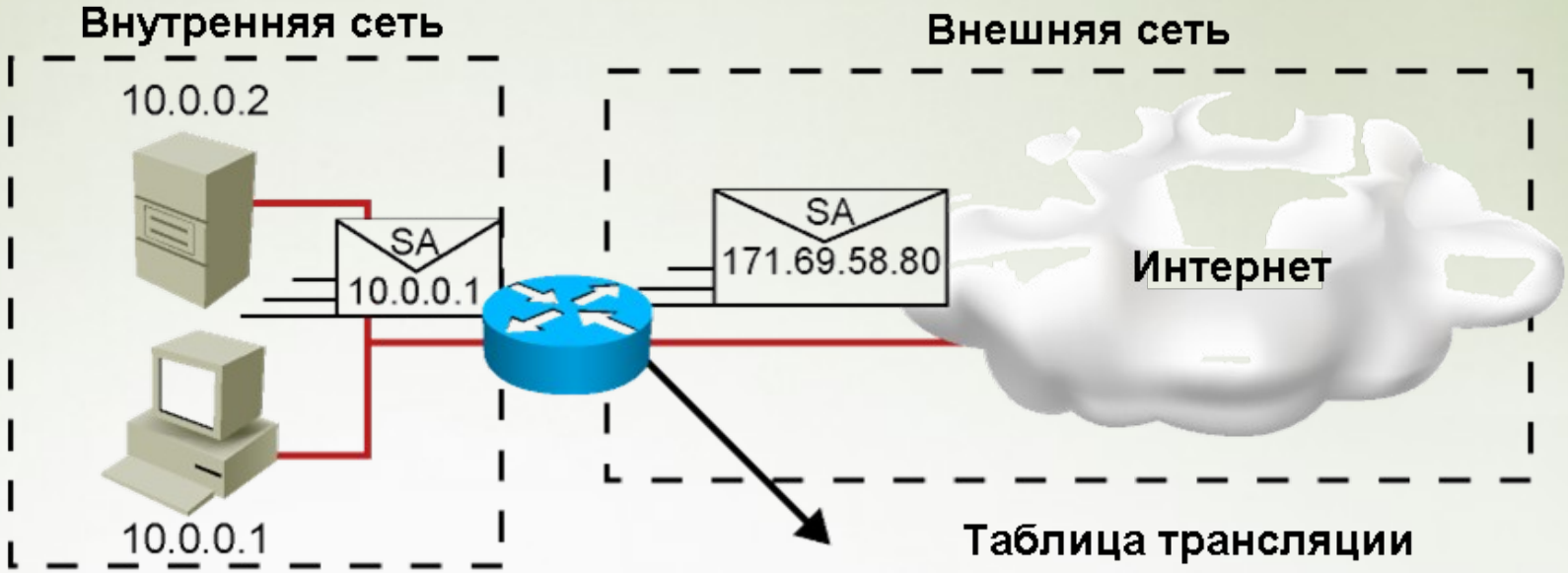


Таблица трансляции

Внутренний локальный адрес	Внутренний глобальный адрес
10.0.0.1	171.69.58.80
10.0.0.2	171.69.58.81

301P_175

- IP адрес может быть либо локальным, либо глобальным
- Локальные адреса используется внутри локальных сетей
- Глобальные адреса используются для пересылки трафика в глобальных сегментах сети

PAT: Port Address Translation

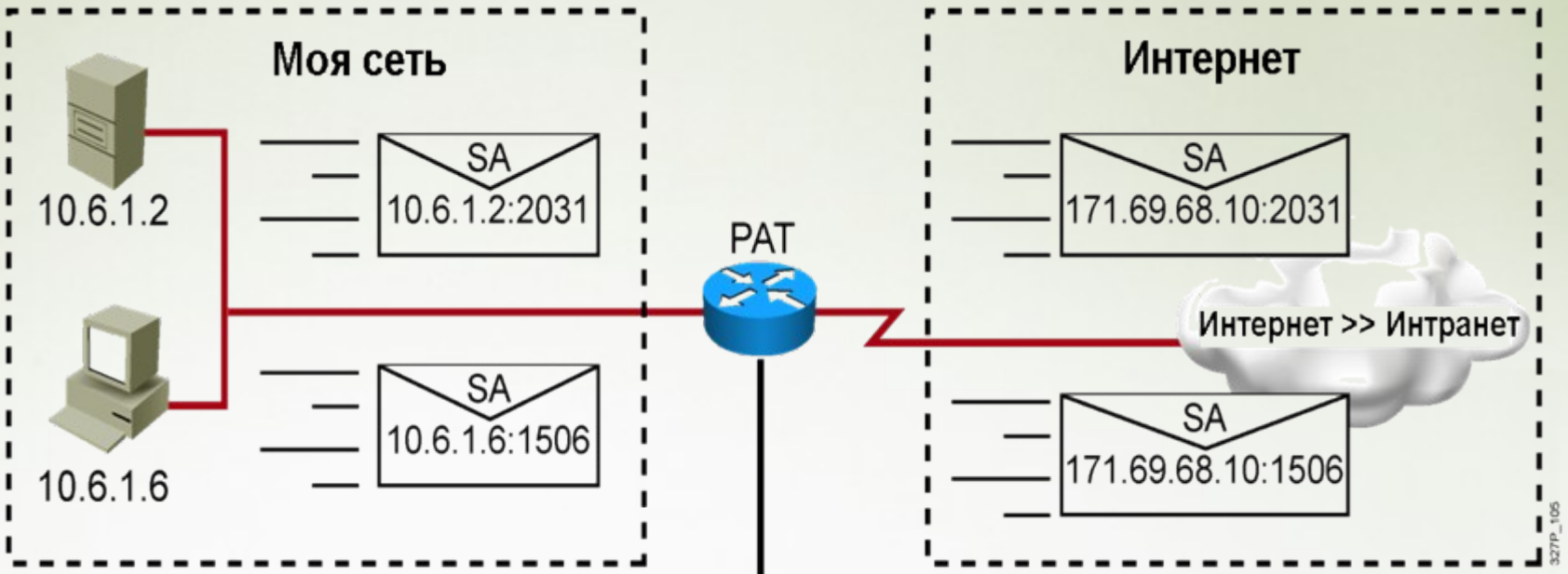
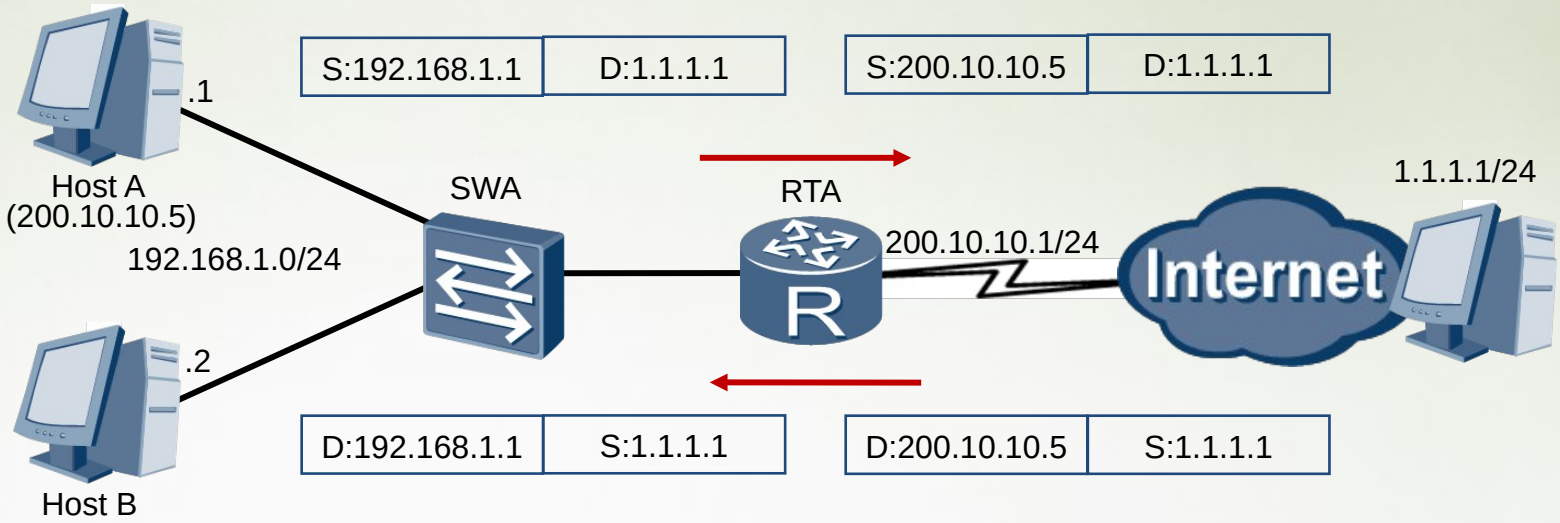


Таблица трансляции

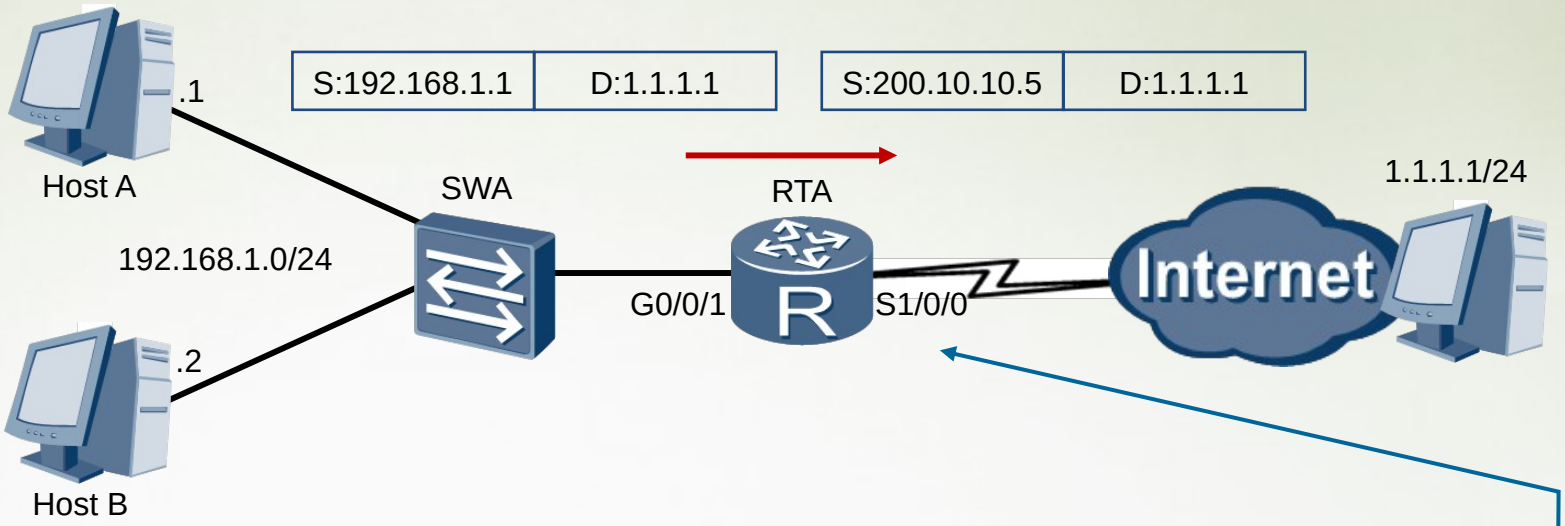
Внутренний локальный адрес	Внутренний глобальный адрес
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506
10.6.1.6:131	171.69.68.10:2032

Статический NAT



Один приватный адрес транслируется в один публичный адрес

Настройка статической трансляции



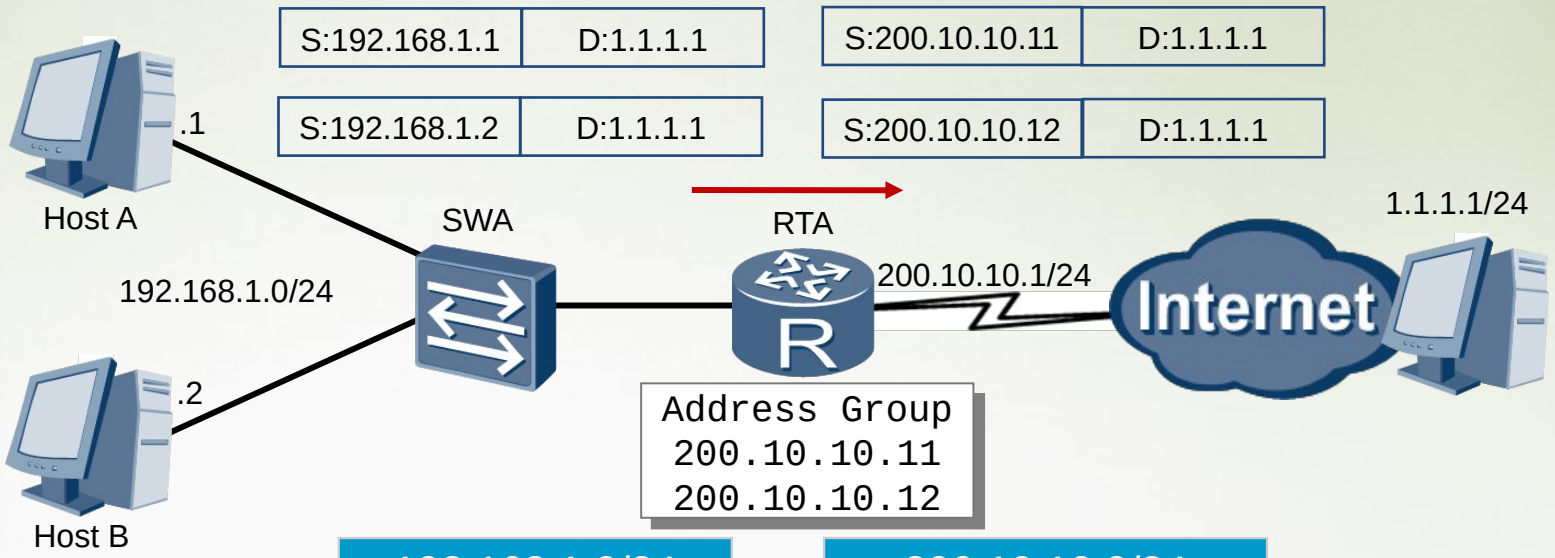

```
[RTA]interface GigabitEthernet0/0/1
[RTA-GigabitEthernet0/0/1]ip address 192.168.1.254 24
[RTA]interface Serial1/0/0
[RTA-Serial1/0/0]ip address 200.10.10.1 24
[RTA]nat static global 200.10.10.5 inside 192.168.1.1
```

Проверка настройки статического NAT

```
[RTA]display nat static
  Static Nat Information:
  Interface  : Serial1/0/0
    Global IP/Port     : 200.10.10.5/----
    Inside IP/Port     : 192.168.1.1/----
    Protocol : ----
    VPN instance-name  : ----
    Acl number         : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    1
```

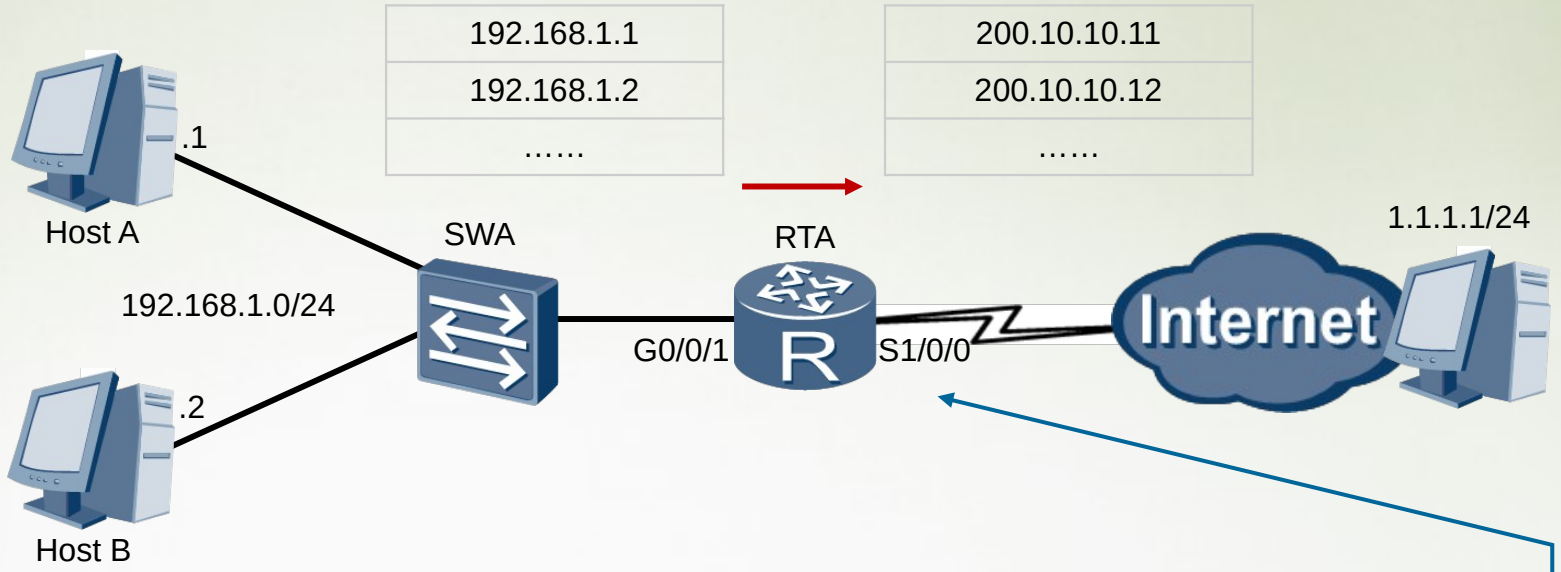
Динамический NAT



192.168.1.0/24	200.10.10.0/24
192.168.1.1	200.10.10.11
192.168.1.2	200.10.10.12

Трансляция основана на использовании пула публичных адресов

Настройка динамического NAT

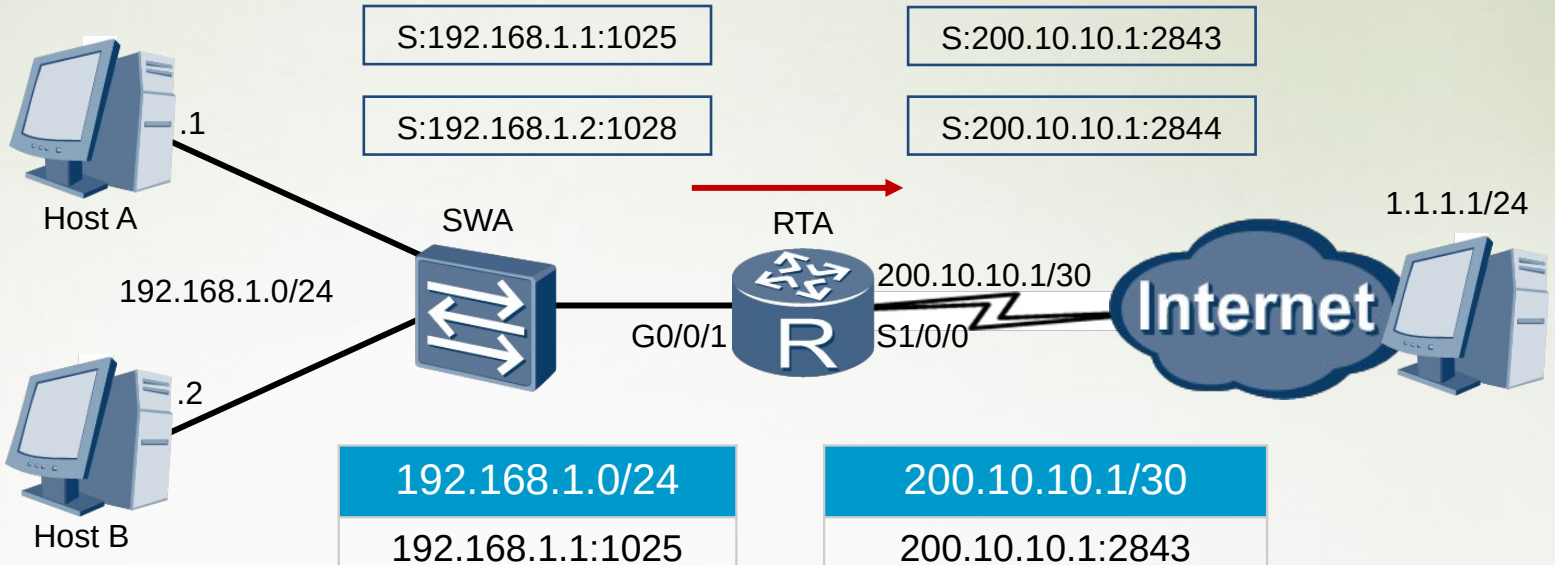



```
[RTA]nat address-group 1 200.10.10.11 200.10.10.16
[RTA]acl 2000
[RTA-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000]quit
[RTA]interface serial1/0/0
[RTA-Serial1/0/0]nat outbound 2000 address-group 1 no-pat
```

Проверка настройки динамического NAT

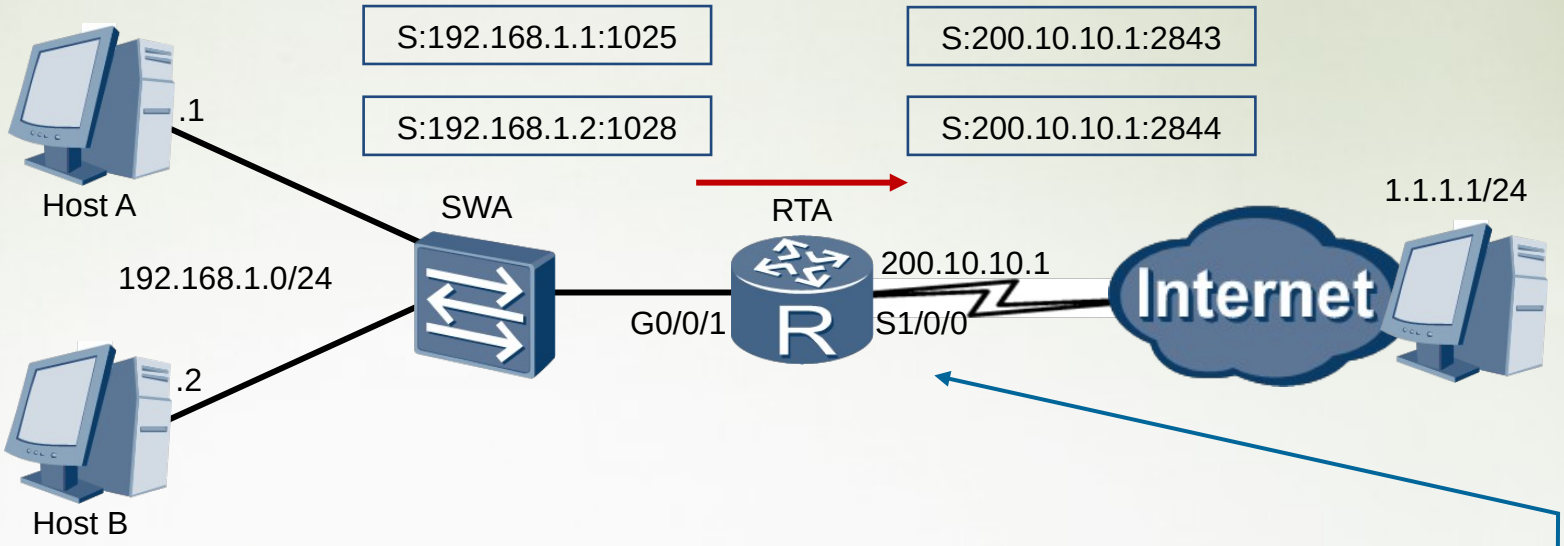
```
[RTA]display nat address-group 1
 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 1       200.10.10.11       200.10.10.16
[RTA]display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------
 Interface           Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------
 Serial1/0/0       2000                          1         no-pat
 --------------------------------------------------------------------
  Total : 1
```

Вариант NAT с трансляцией портов — Easy IP



IP- адрес интерфейса, которым маршрутизатор подключается к публичной сети, используется как единственный публичный адрес для всех устройств в приватной сети. Для того, чтобы отличать сессии, используются номера портов.

Настройка Easy IP




```
[RTA]acl 2000
[RTA-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000]quit
[RTA]interface serial1/0/0
[RTA-Serial1/0/0]nat outbound 2000
```

Проверка настройки Easy IP

```
[RTA] display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface         Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 Serial1/0/0       2000      200.10.10.1                   easyip
 --------------------------------------------------------------------------
  Total : 1
```

Вопросы?