Архитектура вычислительных систем

Лекция 4. Сетевой слой
Часть 2

Artem Beresnev

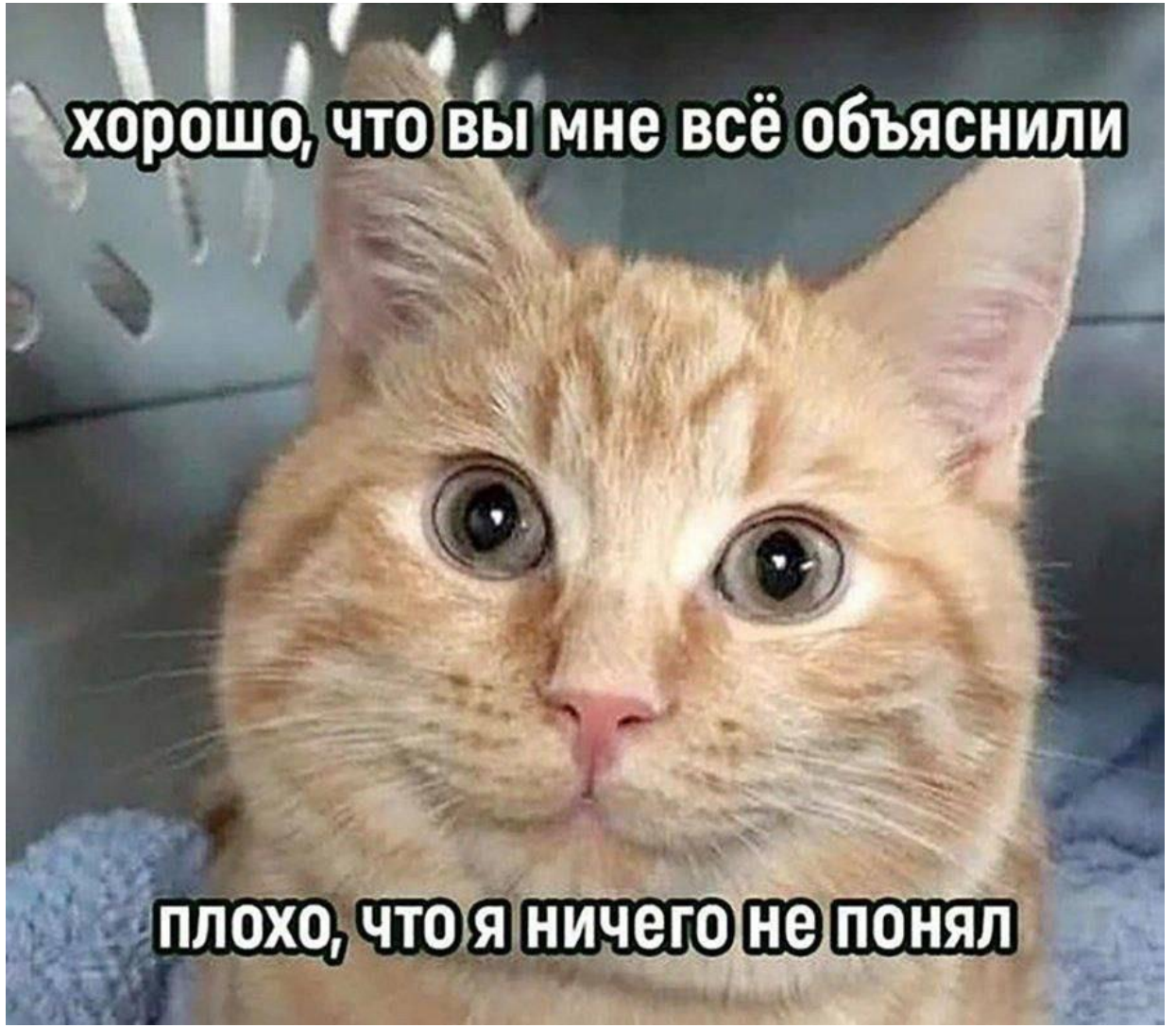
t.me/ITSMDao

t.me/ITSMDaoChat

План

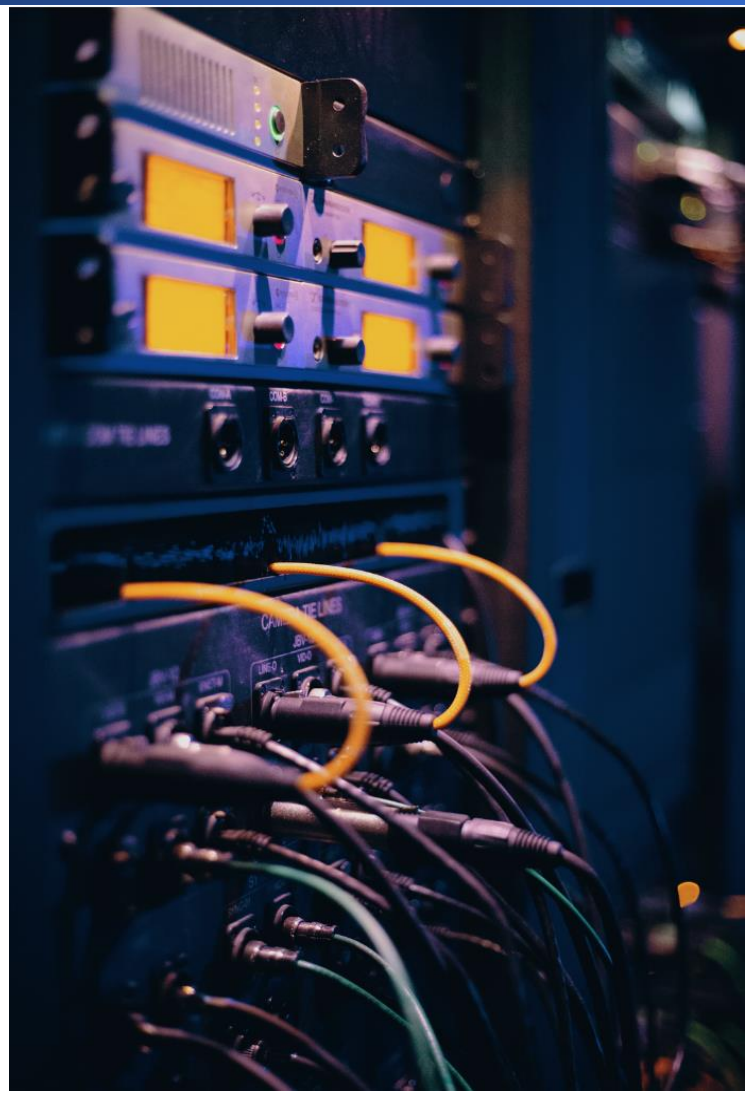
- Вспомним задачи слоя Network и основные принципы
- Вспомним IPv4 адресацию
- NAT
- SSH

Будьте смелыми котиками

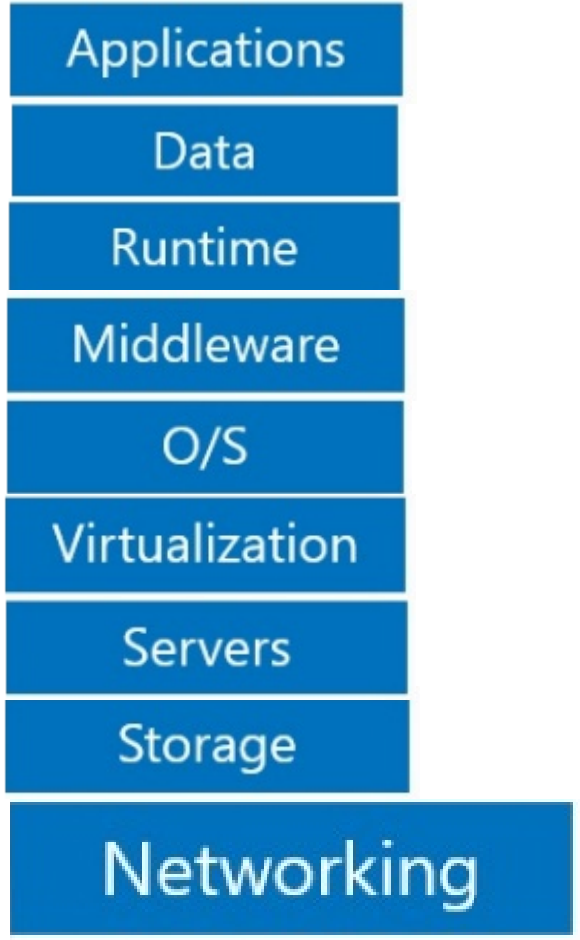


Вспомним, что мы уже знаем про слой Networking

И основные понятия



ИТ-инфраструктура

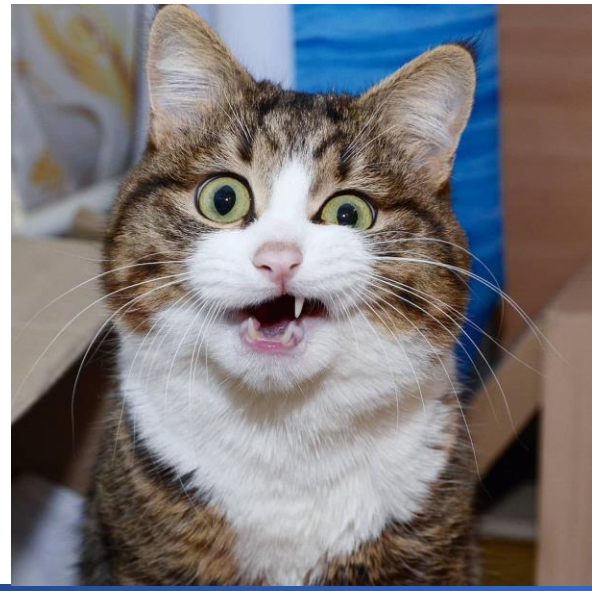


Networking – сетевая инфраструктура.
Этот слой предоставляет сетевые ресурсы и услуги, обеспечивающие соединение, маршрутизацию и безопасность данных.

Проблемы сетевой коммуникации

Невозможность реализации коммуникации в рамках монолитных и проприетарных систем

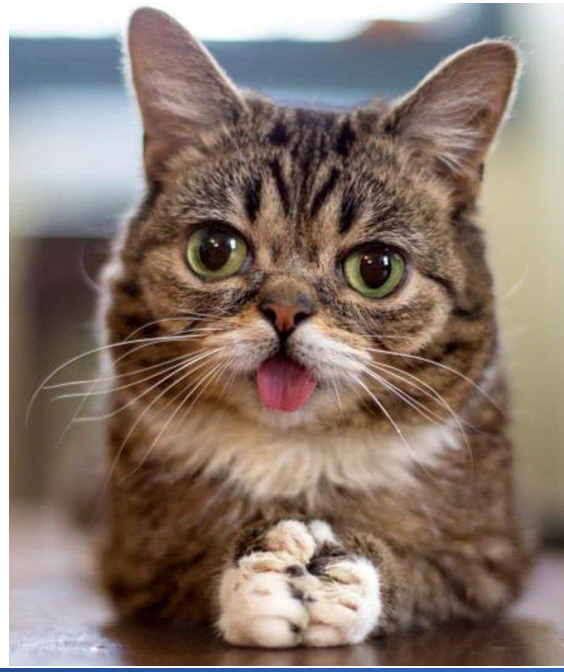
Потребность общедоступных, совместимых стандартах, обеспечивающих сетевую коммуникацию на основе использования совместимых и (или) взаимозаменяемых компонентов



Сетевой стек

Сетевой стек – набор сетевых протоколов, работающих в определенной последовательности с целью передачи данных по компьютерной сети между двумя и более системами (возможен и частный случай взаимодействия различных приложений через сетевой стек в пределах одной системы).

Протокол – соглашение об обработке данных и интерфейсах ввода-вывода, используемое для реализации модуля, решающего подзадачу сетевой коммуникации в рамках общей задачи сетевого взаимодействия.



Стек TCP\IP

Прикладной уровень

Транспортный уровень

Сетевой уровень

Канальный уровень

Дейтаграммная передача

Адресация на разных уровнях

Уровень стека	Адрес	Пример
Прикладной уровень	DNS, X.500, WINS условно	www.ifmo.ru
Транспортный уровень	Номер порта TCP или UDP	443
Сетевой уровень	Ip адрес	192.168.0.103 fe80::59e1:d46b:1bb:5169
Канальный уровень	Media Access Control (MAC)	BC:EE:7B:5B:E5:E5

Синтетические адреса: URL, socket (ip:port)

Установление соединения

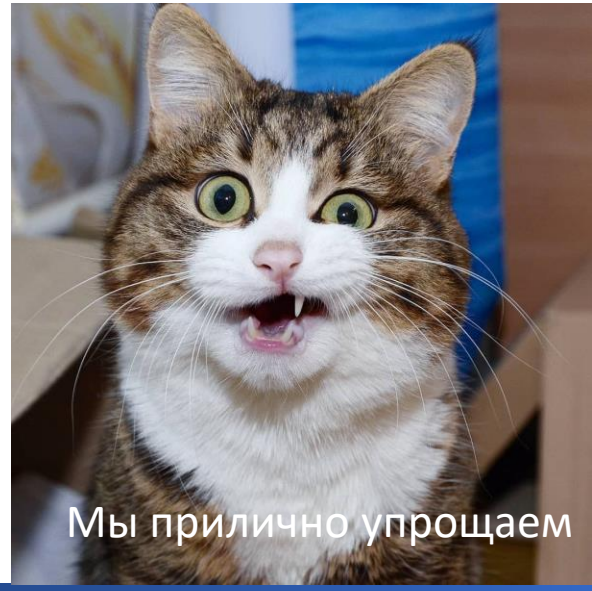
- Цель установить соединение между программой-клиентом и программой-сервером.
- Первичная конфигурация:
  - Назначаем IP адреса для компьютеров (предполагаем что маршрутизация работает)
  - Программа сервер при запуске занимает порт (пусть TCP). Номер порта известен заранее.
  - Программа клиент при запуске занимает свободный порт выше 1024.

Web-browser
TCP 29384

Web-server
TCP 80

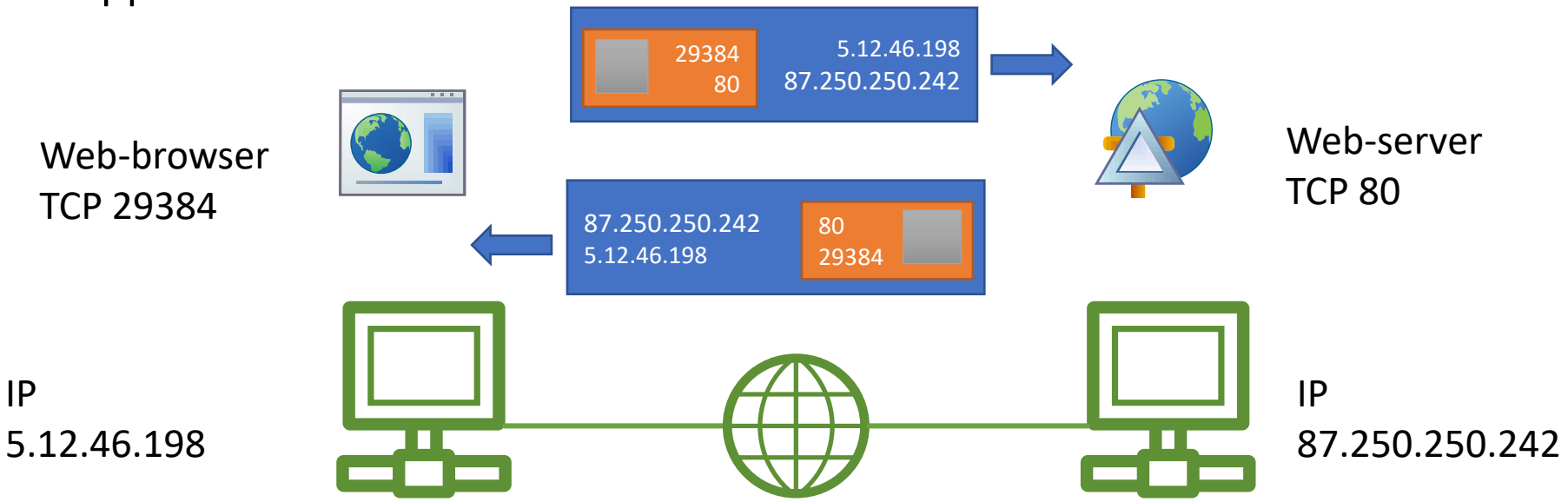
IP
5.12.46.198

IP
87.250.250.242

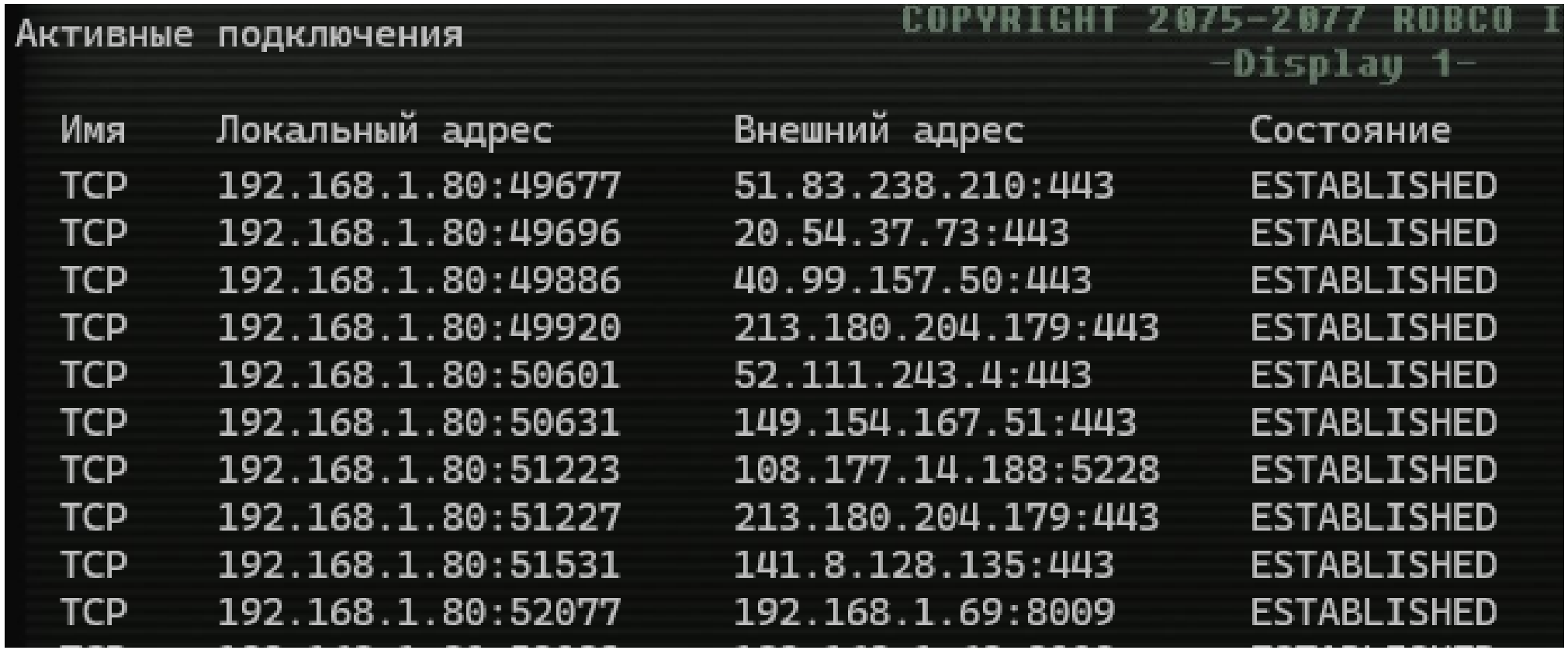


Установление соединения

- Программа клиент передает модулям TCP и IP информацию о номере порта и адресе назначения.
- Передаются данные первого пакета (указывается номер порта отправителя и адрес отправителя).
- Целевой компьютер получает информацию и отвечает на запрос.
- Устанавливается соединение
- Передаются данные.

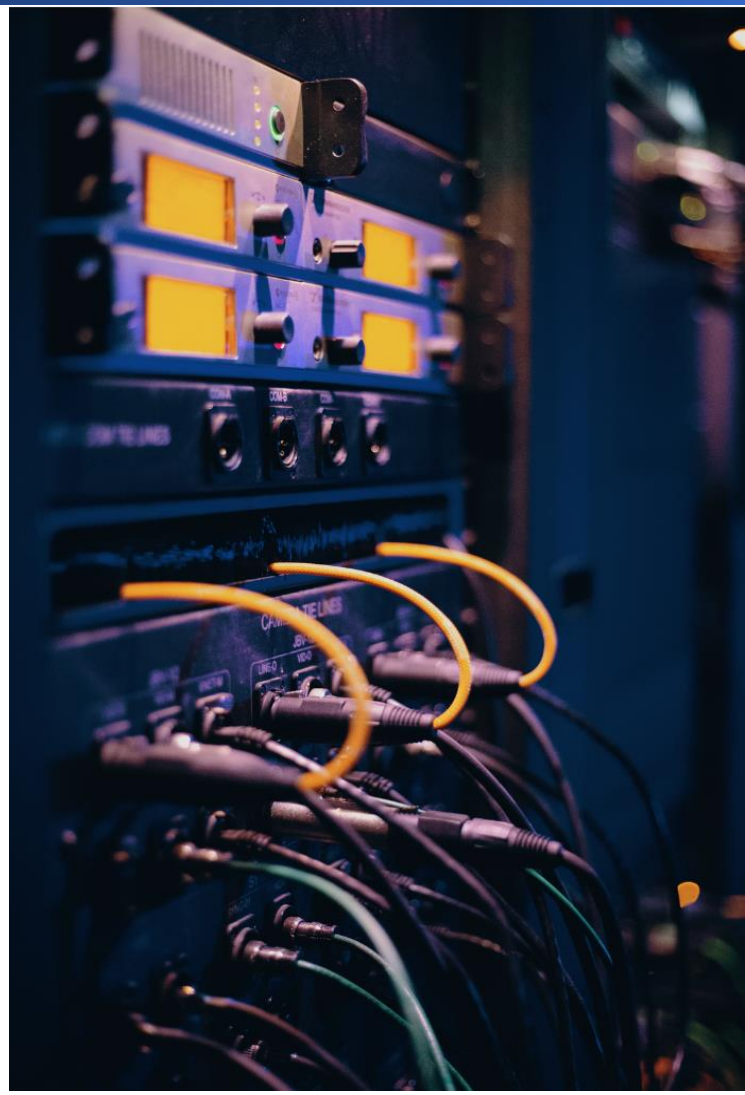


Соединения


Активные подключения
COPYRIGHT 2075-2077 ROBCO I
-Display 1-
Имя Локальный адрес Внешний адрес Состояние
TCP 192.168.1.80:49677 51.83.238.210:443 ESTABLISHED
TCP 192.168.1.80:49696 20.54.37.73:443 ESTABLISHED
TCP 192.168.1.80:49886 40.99.157.50:443 ESTABLISHED
TCP 192.168.1.80:49920 213.180.204.179:443 ESTABLISHED
TCP 192.168.1.80:50601 52.111.243.4:443 ESTABLISHED
TCP 192.168.1.80:50631 149.154.167.51:443 ESTABLISHED
TCP 192.168.1.80:51223 108.177.14.188:5228 ESTABLISHED
TCP 192.168.1.80:51227 213.180.204.179:443 ESTABLISHED
TCP 192.168.1.80:51531 141.8.128.135:443 ESTABLISHED
TCP 192.168.1.80:52077 192.168.1.69:8009 ESTABLISHED

Вспомним основные моменты по адресации IPv4

Да, это было в ЕГЭ.
Правда тогда было здорово? ☺



IP - адресация

IP-адрес – это уникальный числовой адрес, который однозначно идентифицирует узел, группу узлов или сеть.

IPv4-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел «**октетов**», разделенных точками – W.X.Y.Z Каждый октет может принимать значения в диапазоне от 0 до 255.

Структура IP адреса

Адрес СЕТИ – Адрес Узла

Доставка до сети назначения. Т.е. для обеспечения работы составных сетей через маршрутизацию.

Доставка до узла внутри сети

Бесклассовая адресация

IP-адрес

Адрес сети	Адрес узла внутри сети

Маска

1111…..11111	0000…000

Запись:

192.168.0.200 mask 255.255.255.0

или

192.168.0.200/24

Деление с помощью маски

- Пример 1 (192.168.0.0 mask 255.255.255.0 или 192.168.0.0/24)

```
Address:   192.168.0.1          11000000.10101000.00000000. 00000001
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111

Network:   192.168.0.0/24       11000000.10101000.00000000. 00000000
HostMin:   192.168.0.1          11000000.10101000.00000000. 00000001
HostMax:   192.168.0.254        11000000.10101000.00000000. 11111110
Broadcast: 192.168.0.255        11000000.10101000.00000000. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

Деление с помощью маски

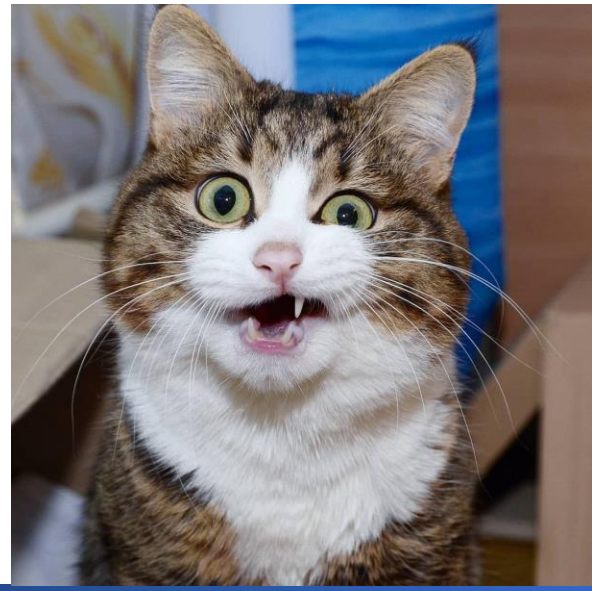
- Пример 2 (192.168.0.0 mask 255.255.255.252 или 192.168.0.0/30)

```
Address:   192.168.0.1           11000000.10101000.00000000.000000 01
Netmask:   255.255.255.252 = 30  11111111.11111111.11111111.111111 00
Wildcard:  0.0.0.3               00000000.00000000.00000000.000000 11

Network:   192.168.0.0/30        11000000.10101000.00000000.000000 00
HostMin:   192.168.0.1           11000000.10101000.00000000.000000 01
HostMax:   192.168.0.2           11000000.10101000.00000000.000000 10
Broadcast: 192.168.0.3           11000000.10101000.00000000.000000 11
Hosts/Net: 2                      Class C, Private Internet
```

Зачем нужно знать маску при настройке?

Зачем знать маску при установке адреса?

- Для определения границ адресов LAN
- Для формальной проверки gateway
- Для организации широковещания



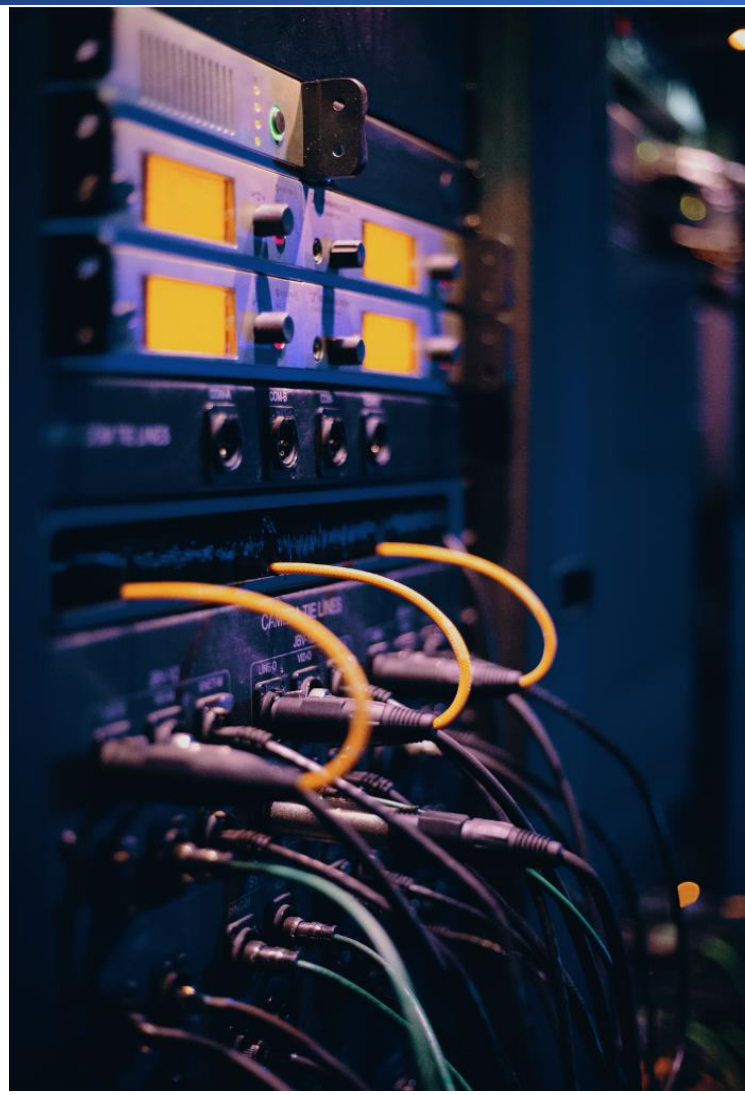
Частные или серые IP-адреса

В соответствии со стандартом RFC 1918 было зарезервировано несколько диапазонов адресов класса A, B и C. Не для Интернета!

A - 10.0.0.0/8	10.0.0.0–10.255.255.255
B - 172.16.0.0/12	172.16.0.0–172.31.255.255
C - 192.168.0.0/16	192.168.0.0–192.168.255.255

Как соединяются сети на основе IP ?

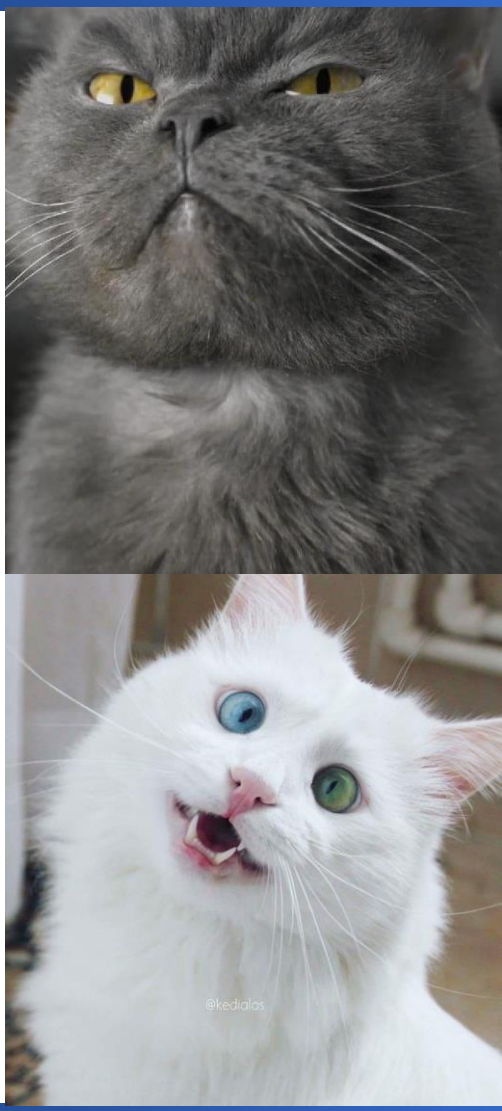
Есть два способа. В современных сетях они используются одновременно.



Итак, два способа соединения IP сетей

Маршрутизация - общее непротиворечивое адресное пространство и видимость из конца-в-конец. В случае Интернета только белые адреса

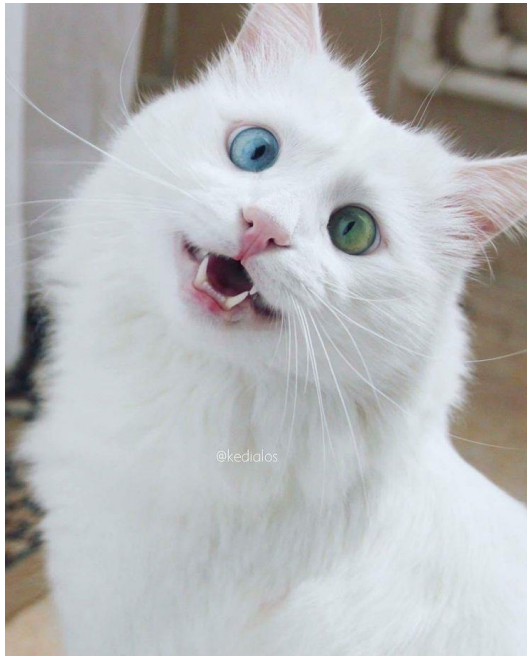
Трансляцию адресов - разделенное адресное пространство, изоляция локальных сетей (нет видимости из конца-в-конец). В случае Интернет используются и белые и серые адреса.



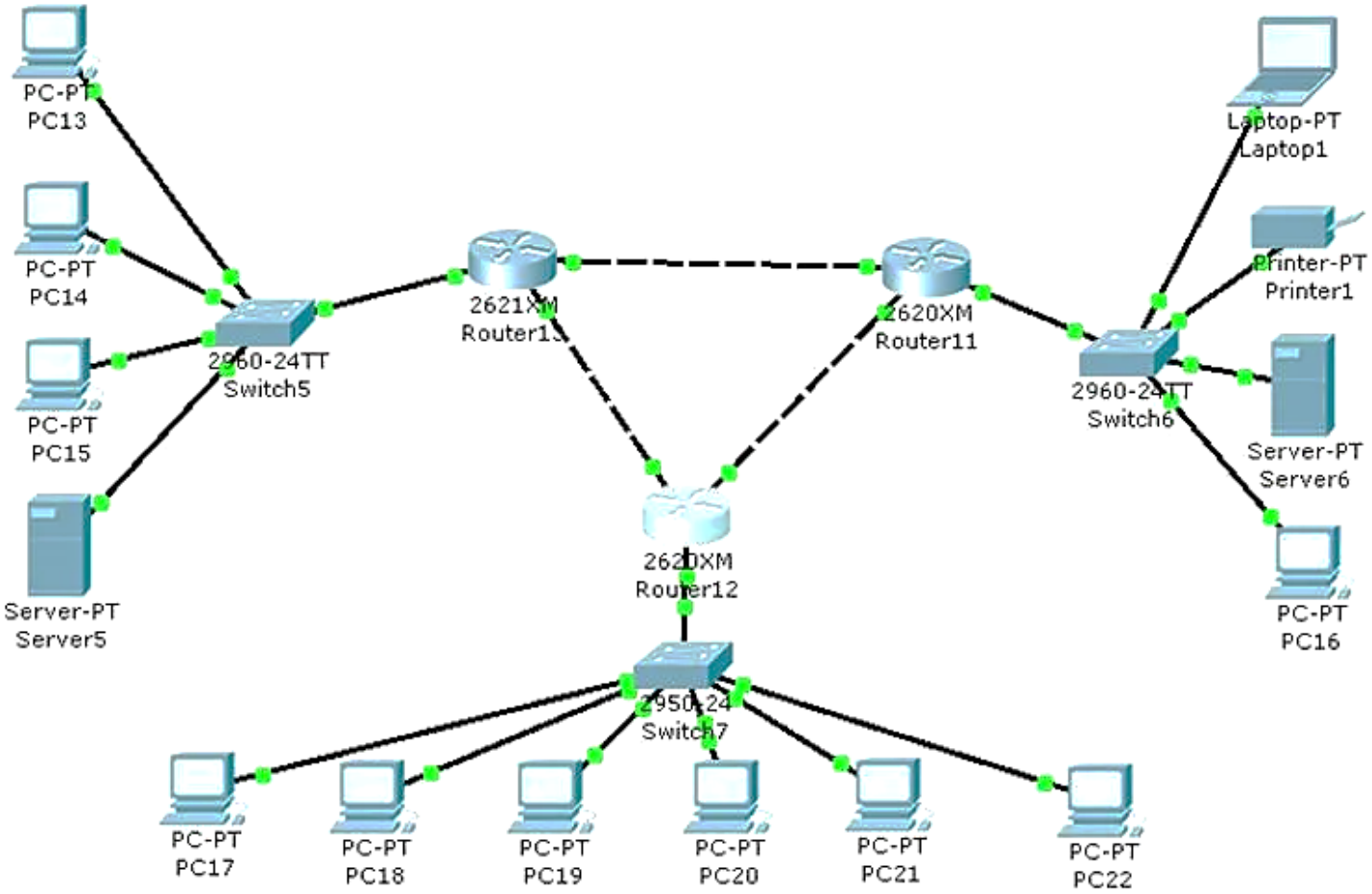
Маршрутизация

Маршрутизация:

1) у каждой локальной сети свой уникальный адрес IP-сети
2) у каждого хоста свой уникальный адрес
3) диапазоны адресов в разных локальных сетях не пересекаются (в Интернет используются белые диапазоны адресов).
4) Между сетями – маршрутизаторы у которых есть таблица маршрутизации. По ней принимается решение о направлении передачи.



Маршрутизация



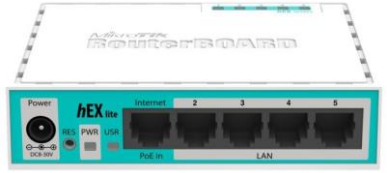
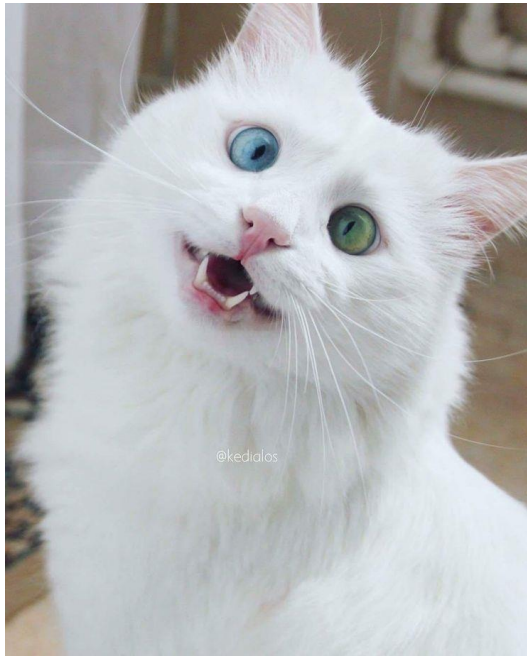


Таблица маршрутизации

```
IPv4 таблица маршрута
===========================================================================

Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.80     35
        127.0.0.0        255.0.0.0         On-link       127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link       127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link       127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link     192.168.1.80    291
     192.168.1.80  255.255.255.255         On-link     192.168.1.80    291
    192.168.1.255  255.255.255.255         On-link     192.168.1.80    291
     192.168.56.0    255.255.255.0         On-link     192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link     192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.1.80    291
  255.255.255.255  255.255.255.255         On-link       127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.1.80    291
===========================================================================

Постоянные маршруты:
  Сетевой адрес           Маска    Адрес шлюза      Метрика
    217.79.12.121  255.255.255.255       10.13.0.1       1
    95.161.179.30  255.255.255.255       10.13.0.1       1
===========================================================================
```



Трансляция адресов или NAT

Трансляция:

1) Цель: обеспечить связь хостов из немаршрутизируемой сети во внешнюю IP сеть
2) IP-адреса локальных сетей независимы и могут повторятся
3) но в локальной сети у каждого хоста свой уникальный адрес
4) между сетями – маршрутизаторы которые на ходу изменяют адреса в IP пакетах и (в ряде случаев) номера портов в заголовках TCP и UPD и ведут «учет» что на что поменяли, для того чтобы вернуть все обратно, когда придет ответ
5) к Интернету обычно так подключаются локальные сети с серыми адресами.

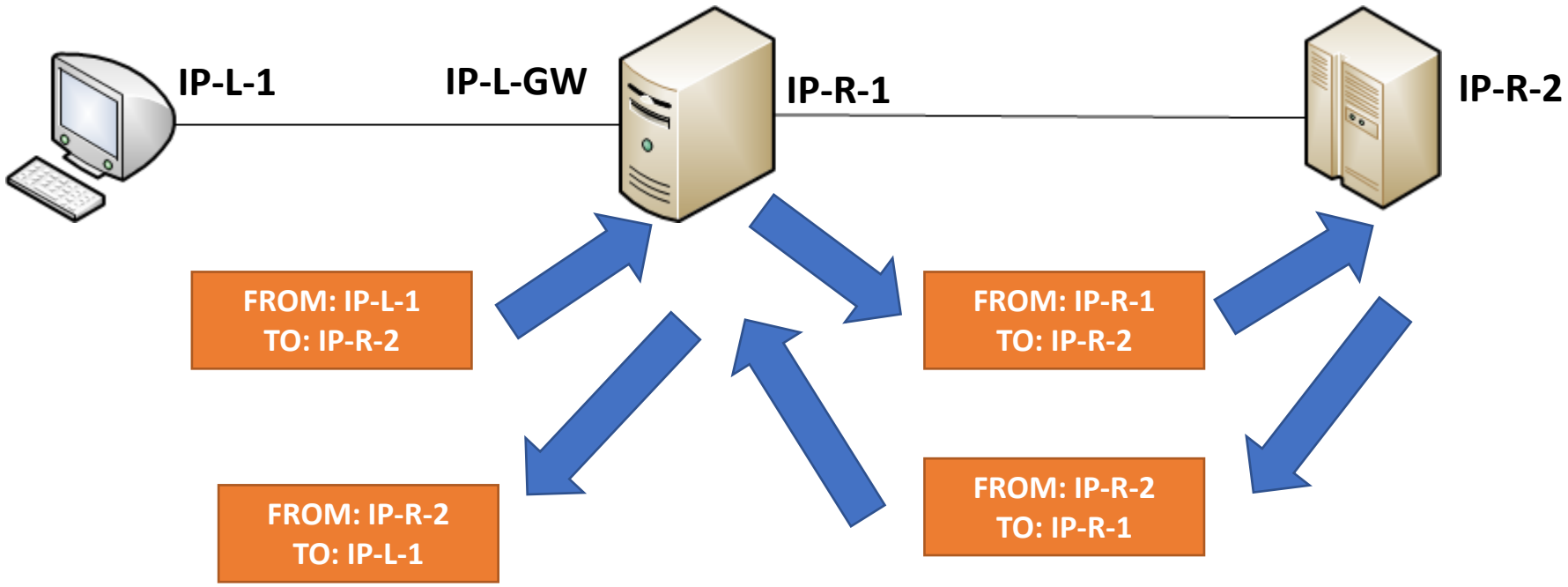
NAT (Network Address Translation)

Виды:

- Публикация адреса
- Клиентский NAT
- Публикация порта

- **Симметричный** - когда все порты внутреннего адреса транслируются на порты внешнего адреса, при этом устройство становится полностью доступным из внешней сети.
- **Динамический** - когда порт внутреннего адреса случайным образом транслируется на порт одного из внешних адресов, причем для каждого нового соединения может быть использован отличающийся адрес
- **Перегруженный** - когда порты нескольких внутренних адресов транслируются на случайные порты единственного внешнего адреса.

Публикация адреса

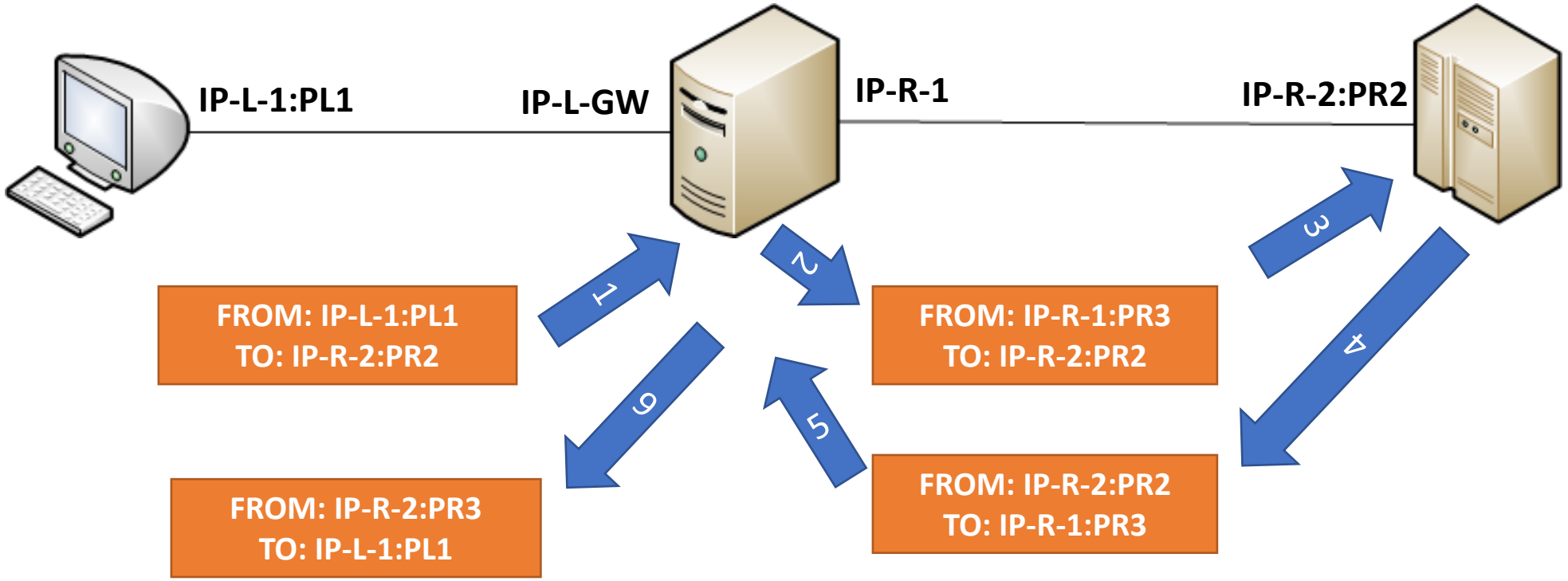


IP-L-1 = IP-R-1

Типичное применение – облачные виртуалки и сервис белого IP

Клиентский NAT

Динамически подменяется не адрес, а сокет отправителя

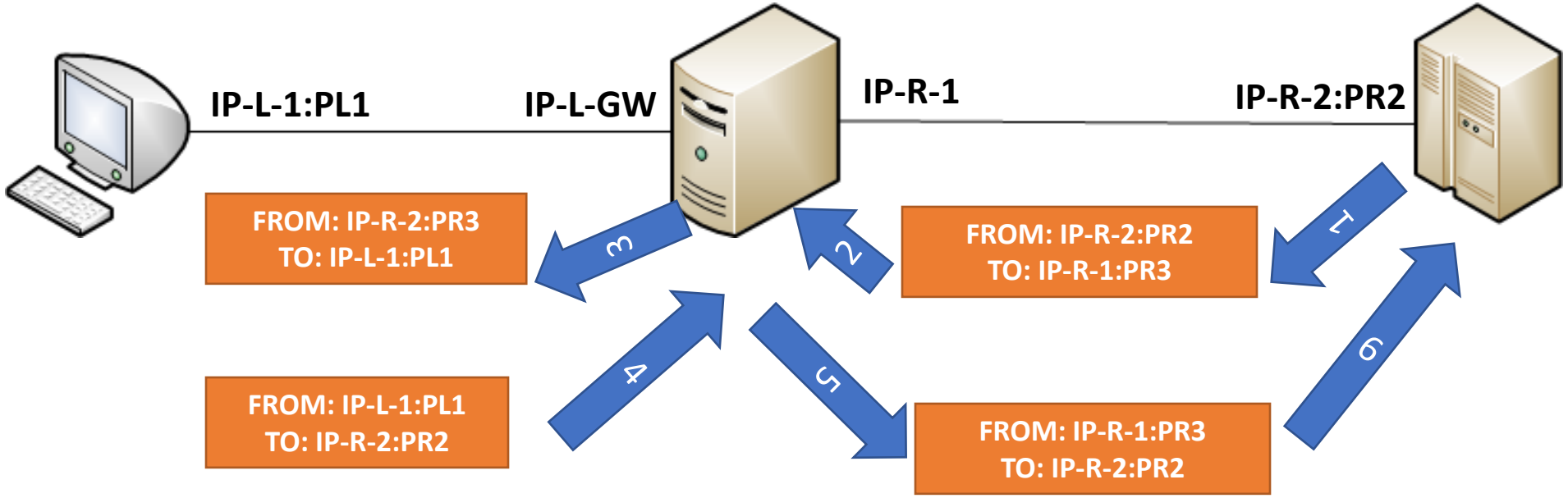


Сокет IP-L-1:PL1 динамически заменен на IP-R-1:PR3

Типичное применение – клиентский доступ во внешнюю сеть

Публикация порта

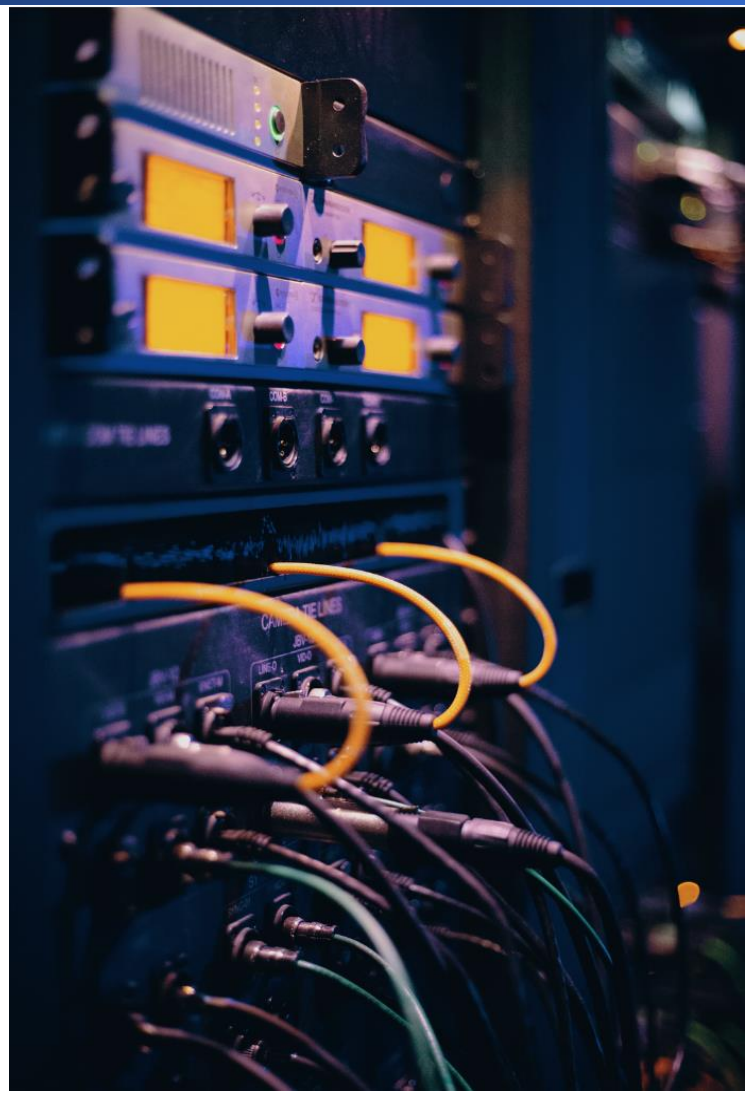
Реальный сокет соотносится с внутренним статически, чтобы можно было подключатся к приложению внутри серой сети снаружи



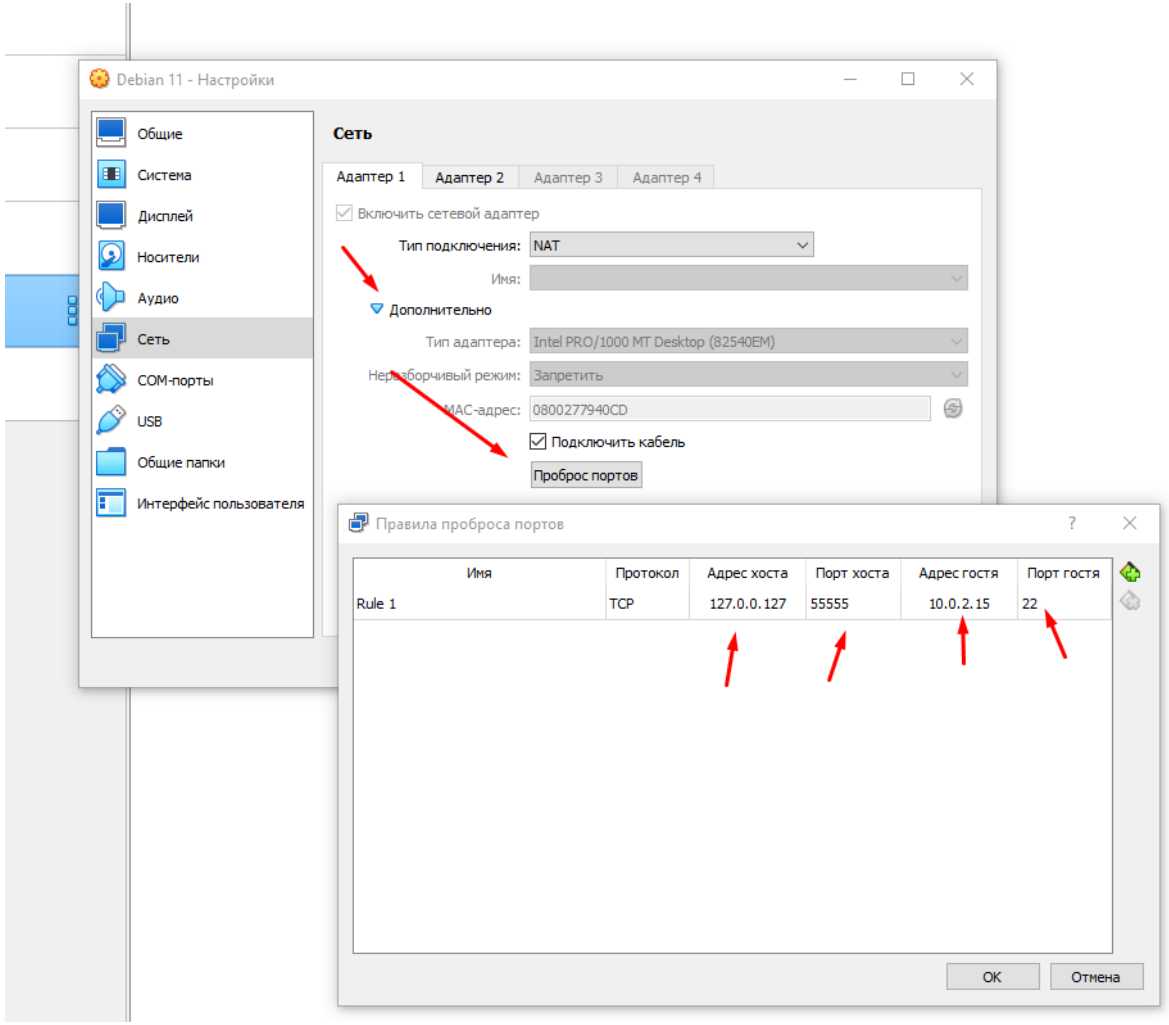
Сокет IP-R-1:PR3 статически отображен на IP-L-1:PL1

Типичное применение – работа сервисов из приватной сети на одном белом IP шлюза.

Немого живых примеров



NAT в VirtualBox и Linux



sysctl -w net.ipv4.ip_forward=1

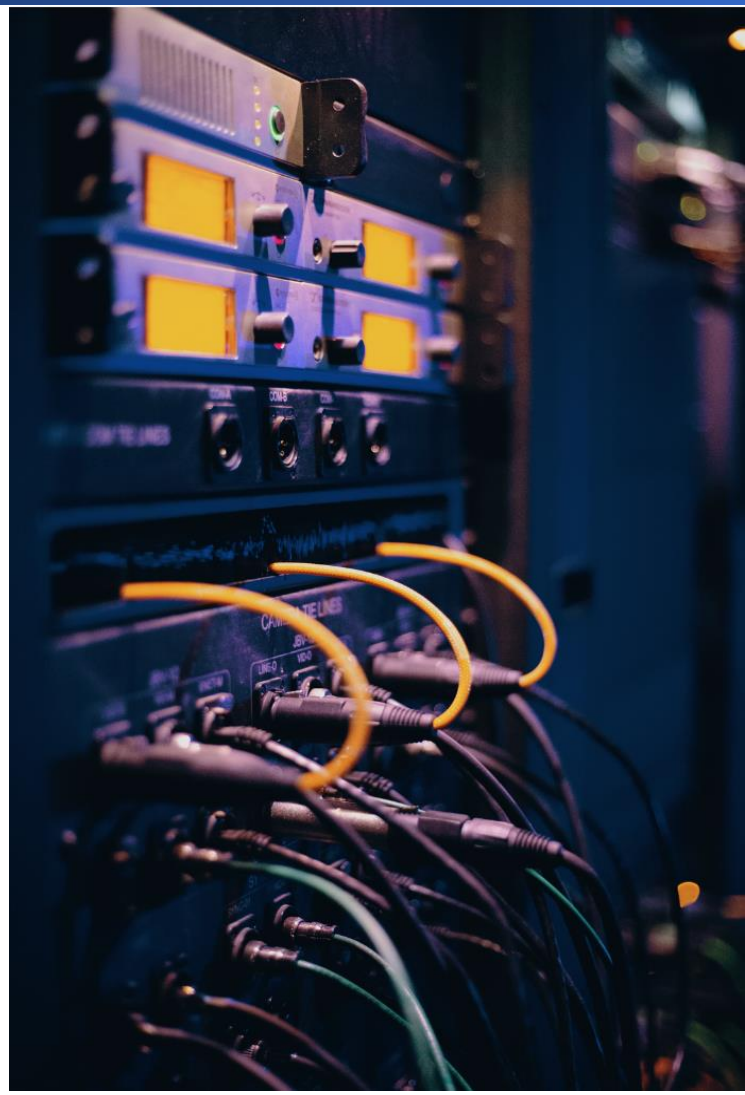
```
iptables -t nat -A POSTROUTING -o ИМЯ-СЕТЕВОГО-ИНТЕРФЕЙСА-NAT -s 10.0.0.0/24 -j MASQUERADE

iptables -A FORWARD -d 10.0.0.0/24 -j ACCEPT

iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
```

```
iptables -t nat -A PREROUTING -i ИМЯ-СЕТЕВОГО-ИНТЕРФЕЙСА-NAT -p tcp --dport 55022 -j DNAT --to-destination 10.0.0.2:22
```

Сохранение правил

```
iptables-save > /etc/iptables/rules.v4
ip6tables-save > /etc/iptables/rules.v6
iptables-restore < /etc/iptables/rules.v4
iptables-persistent
```

Итоги



Выводы

- Вспомнили про адреса и сокеты
- Узнали о маршрутизации
- Узнали о трансляции адресов
- Узнали как это настроить NAT в среде виртуализации
- Узнали как настроить NAT в Linux