

# Сеть и сетевые протоколы: L3-сеть

Ильмир Сахипов  
Руководитель центра управления сетью АО “Уфанет”



# Ильмир Сахипов

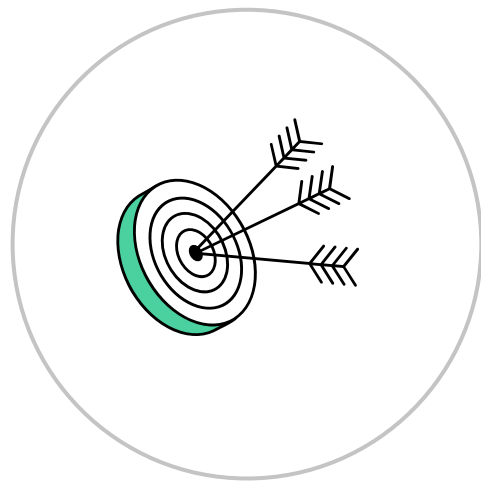
О спикере:

- Руководитель центра управления сетью АО “Уфанет”
- Более 10 лет опыта в области телекоммуникаций
- Эксперт в решении сложных клиентских и сетевых инцидентов на мультивендорной мультисервисной операторской сети



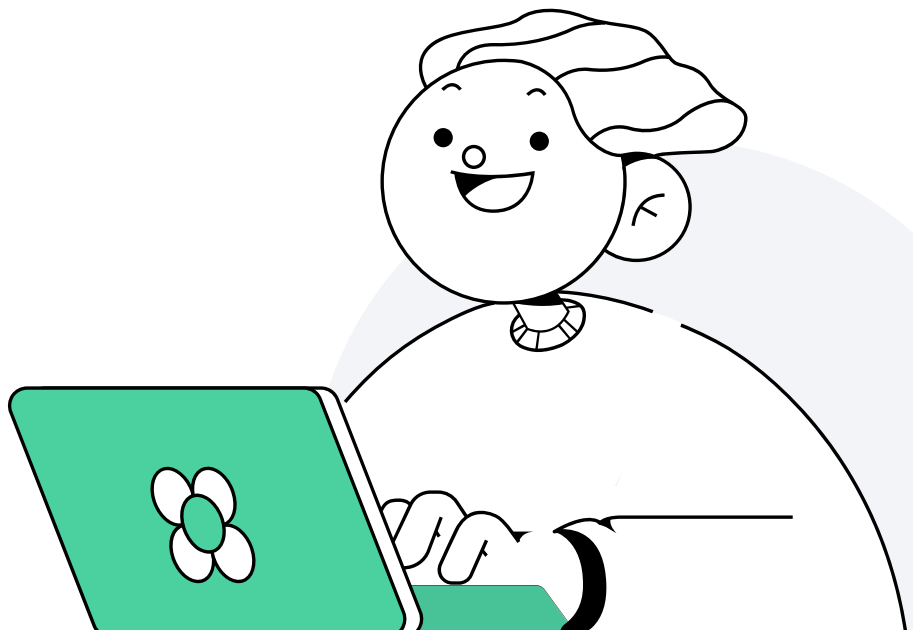
# Цели занятия

- Разобрать основы работы сетевого уровня модели OSI
- Изучить протокол IPv4: возможности, ограничения и особенности адресации
- Познакомиться с протоколом IPv6 и понять его ключевые отличия от IPv4
- Понять особенности маршрутизации в сетях на уровне L3 на примере работы роутера
- Научиться строить статический и динамический маршруты
- Научиться работать с сетевыми утилитами для диагностики и настройки сетей на уровне L3

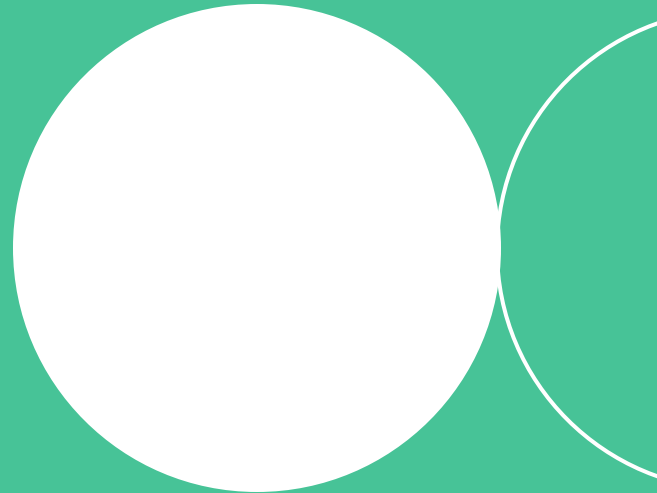


# План занятия

- 1 [Сетевой уровень L3 в модели OSI](#)
- 2 [Обзор протокола IPv4](#)
- 3 [IPv4: адресация](#)
- 4 [IPv4: маска и специальные адреса](#)
- 5 [IPv6](#)
- 6 [Работа маршрутизатора](#)
- 7 [Маршрутизация](#)
- 8 [Популярные сетевые утилиты](#)
- 9 [Итоги занятия](#)
- 10 [Домашнее задание](#)

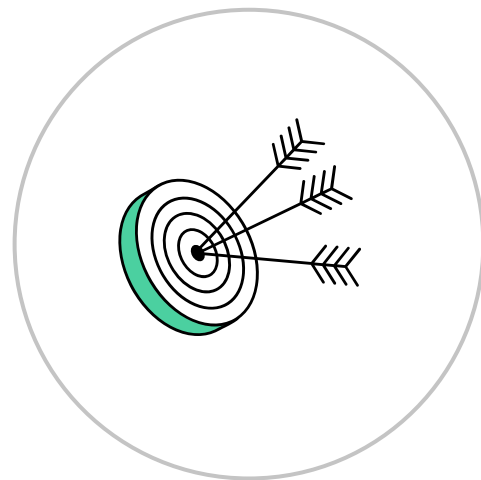


# Сетевой уровень L3 в модели OSI



# Цель темы

- Познакомиться с основами работы сетевого уровня в модели OSI



# Уровни модели OSI

**Прикладной уровень**

Application layer

**Уровень представления**

Presentation layer

**Сеансовый уровень**

Session layer

**Транспортный уровень**

Transport layer

**Сетевой уровень**

Network layer

**Канальный уровень**

Data link layer

**Физический уровень**

Physical layer

Определяет способы передачи данных между устройствами, находящимися в разных сетях (сегментах сети)

# Сетевой уровень: решаемые проблемы

- Логическая адресация
- Построение маршрутов между сетями
- Диагностика сети



# Сетевой уровень: единица данных



пакет

# Сетевой уровень: примеры оборудования и протокола



Маршрутизатор

IPv4, IPv6, ICMP

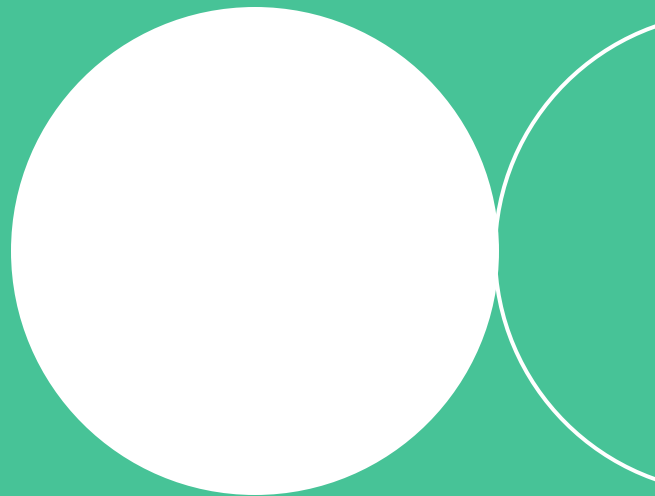
# **Сетевой уровень: пример схемы работы**

# Итоги темы

- 1 Сетевой уровень - это третий уровень в модели OSI, который отвечает за обмен данными между устройствами в разных сетях / сегментах сети
- 2 Ключевое оборудование на L3 - маршрутизатор и протоколы IPv4 и IPV6

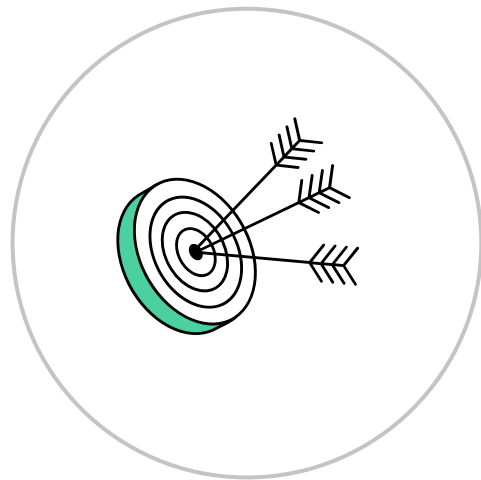


# Обзор протокола IPv4



# Цели темы

- Познакомиться с протоколом IPv4, его назначением и форматом метаданных IP-пакета
- Изучить ограничения IPv4, причины их возникновения и влияние на сети TCP/IP



# Два типовых адреса сети

1

**L2 MAC**

**для адресации внутри  
локальной сети**

(шестнадцатеричная  
запись)

2

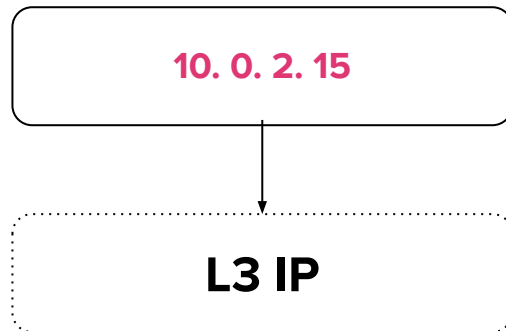
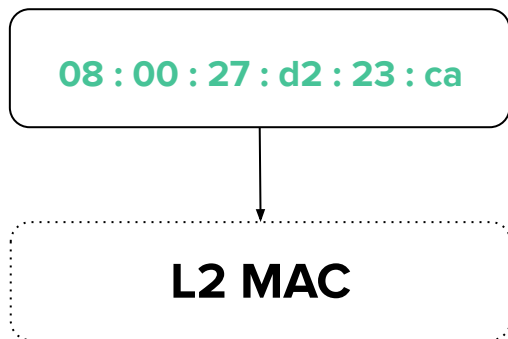
**L3 IP**

**для адресации между  
сетями**

(десятичная запись)

# L2 MAC и L3 IP присутствуют одновременно

```
vagrant@netology1:~$ ip addr show eth0 | egrep '(ether|inet )'  
link/ether 08:00:27:d2:23:ca brd ff:ff:ff:ff:ff:ff  
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
```





# Общение приложений по спецификациям TCP/IP



**TCP + MAC**



**TCP + IP**



**Как хост «понимает», что  
адрес сетевого уровня  
относится / не относится  
к его собственной сети?**



## Маска подсети

**битовая маска для определения по IP-адресу адреса подсети и адреса узла (хоста, компьютера, устройства) этой подсети**





## IP (Internet Protocol)

**СОЗДАН ДЛЯ ИСПОЛЬЗОВАНИЯ ВО  
ВЗАИМОСВЯЗАННЫХ СИСТЕМАХ  
КОМПЬЮТЕРНЫХ СЕТЕЙ С КОММУТАЦИЕЙ  
ПАКЕТОВ**



# К чему относится IPv4?



# Стандарт протокола IP



RFC 791

# Формат заголовков IPv4

## IPv4 Packet Header Format

Bit #	0	7	8	15	16	23	24	31
0	Version	IHL	DSCP	ECN	Total Length			
32	Identification				Flags	Fragment Offset		
64	Time to Live		Protocol		Header Checksum			
96	Source IP Address							
128	Destination IP Address							
160	Options (if IHL > 5)							

# Назначение IPv4

- Логическая адресация хостов на основе IP-адреса
- Инкапсуляция данные вышестоящих протоколов
- Маршрутизация данных между хостами
- Фрагментация IP-пакетов



# Ограничения IPv4

- не устанавливает соединения
- не гарантирует доставку
- не обеспечивает обеспечения  
сохранение последовательности  
данных при передаче
- не устраняет возможное  
дублирование пакетов



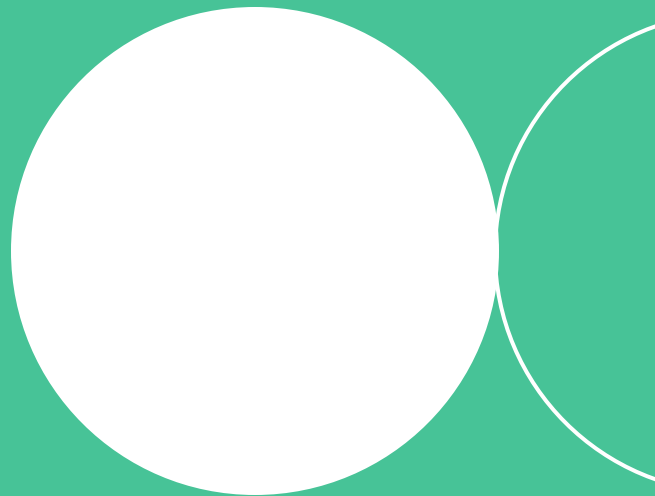
**Решение**  
Протоколы  
транспортного уровня L4

# Итоги темы

- 1 Для установления соединения в сетях TCP/IP используются IP адреса, которые существуют параллельно с L2 MAC-адресам
- 2 Заголовок IP содержит различные параметры и флаги, важнейшими из которых являются адреса отправителя и получателя, и указатель вышестоящего протокола
- 3 Протокол IPv4 служит только для адресации, маршрутизации и фрагментации данных по пакетам. Контролем, сборкой и созданием соединения занимаются вышестоящие протоколы

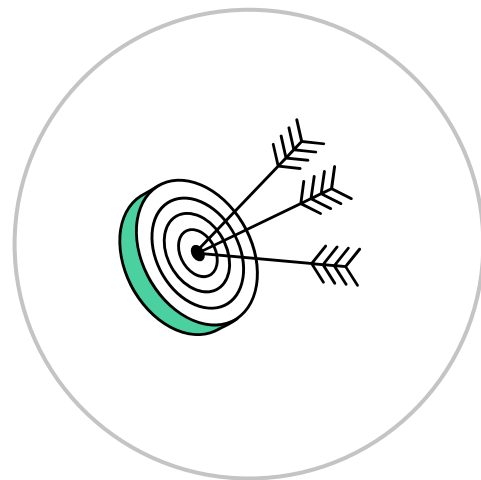


# IPv4: адресация

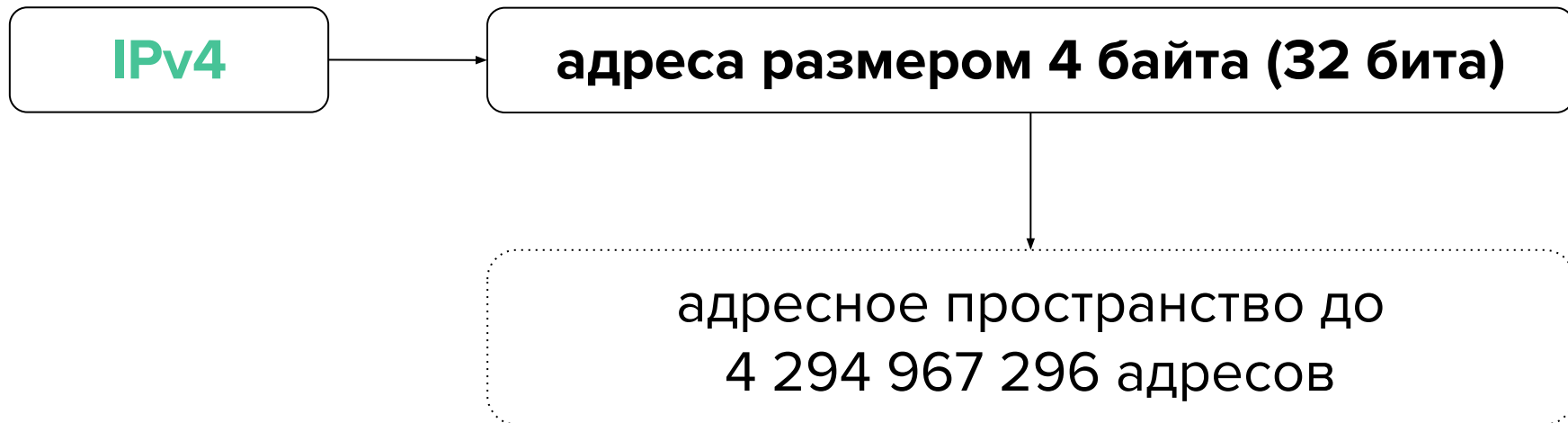


# Цели темы

- Узнать о разделении внутри IP адреса необходимым для маршрутизации
- Разобрать подходы к адресации на уровне L3



# Ограничения адресации

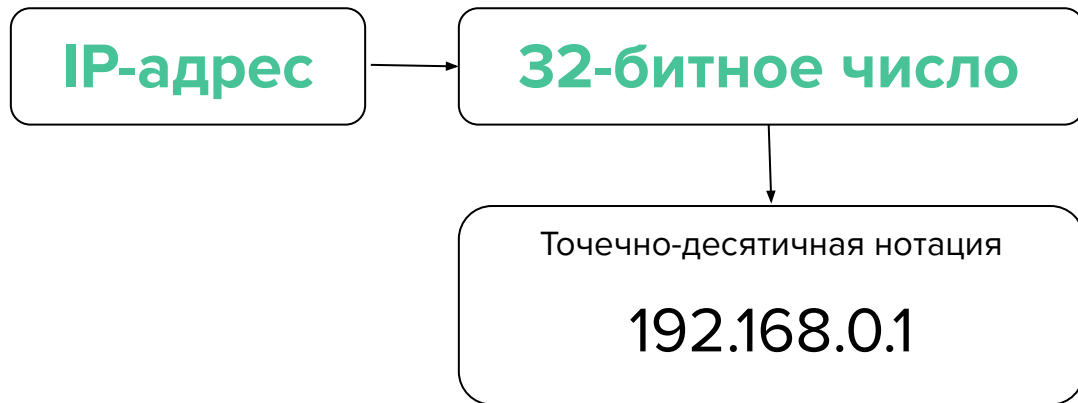




**Последний блок IP-адресов  
был выделен**

**3 февраля 2011 года**

# IP-адрес



# IP-адрес состоит из двух частей

1

**Адрес хоста**

его сетевого  
интерфейса

2

**Адрес сети**

«путь» к хосту  
в сети



# Адресация

Изначально под адрес сети отводился только старший октет и оставшаяся часть представляла из себя адрес хоста:  
**192.0.0.1**

Позже была введена **классовая адресация**, при которой старший октет определял тип адреса сети и количество хостов

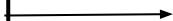
В 1993 году появилась **бесклассовая адресация**, где стало возможным применение любых масок подсети к пространству IP-адресов

# Классовая адресация

класс	первый октет	распределение байт (сеть, хост)	кол-во сетей	кол-во хостов	маска	начальный адрес	конечный адрес
A	0	C.X.X.X	126	16777214	255.0.0.0	1.0.0.0	126.255.255.255
B	10	C.C.X.X	16384	65534	255.255.0.0	128.0.0.0	191.255.255.255
C	110	C.C.C.X	2097152	254	255.255.255.0	192.0.0.0	223.255.255.255
D	1110	multicast (групповой адрес)				224.0.0.0	239.255.255.255
E	11110	резерв				240.0.0.0	255.255.255.255

# Дословный перевод CIDR

Classless Inter-Domain  
Routing



бесклассовая  
междоменная  
маршрутизация



## CIDR

**метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации, возможно применение различных масок подсетей к различным подсетям**



# IPv4 маска, форматы записи

```
vagrant@vagrant:~$ ip -4 addr show eth0
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group  
default qlen 1000
```

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
```

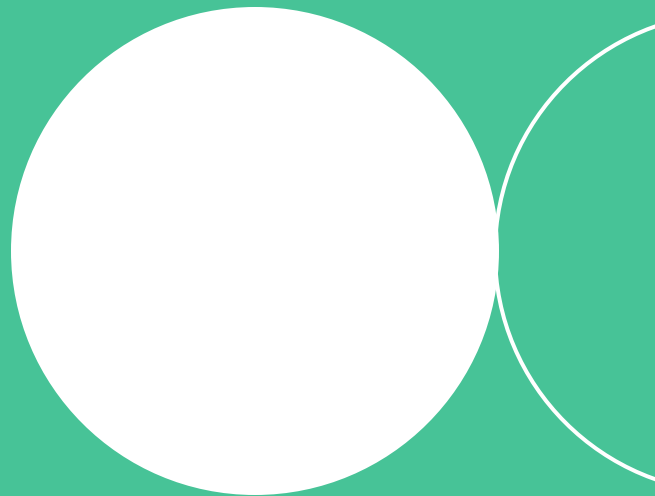
```
valid_lft 49201sec preferred_lft 49201sec
```

# Итоги темы

- 1 Адресов IPv4 всего 4,3 млрд и они уже закончились.  
Для удобства восприятия IP-адрес делится на 4 части, называемые октеты
- 2 Часть в начале IP адреса относится к адресу сети, оставшаяся часть - к адресу хоста в этой сети. Сам IPv4 не содержит указаний по разделению этих частей
- 3 Существовало несколько подходов адресации в сетях L3. Предыдущий вариант назывался классовой адресацией. Он делил сети на 3 класса - А, В и С
- 4 Текущий вариант адресации на уровне L3 называется CIDR, он позволяет гибко делить сети на сегменты

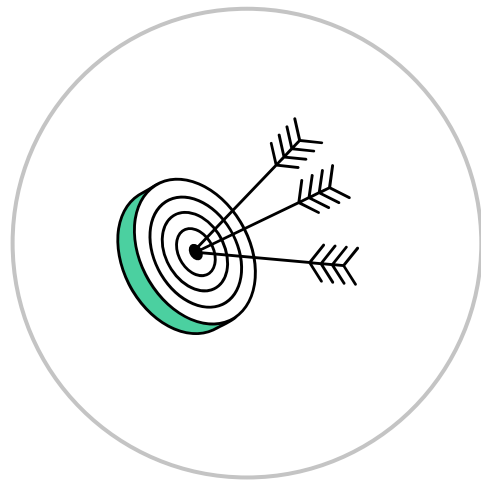


# IPv4: маска и специальные адреса



# Цели темы

- Познакомиться с маской подсети, ее предназначением и формой ее записи
- Узнать, что такое специальные адреса сети, их назначение, способ их определения
- Научиться определять специальные адреса с помощью маски подсети
- Изучить специальные диапазоны IP-адресов







## Маска сети

**количество бит в адресе, которое отведено под  
адрес сети**



# Маска может указываться двумя эквивалентными способами

1

**192.168.0.1/24**

или

2

**255.255.255.0**

из **32 бит** адреса,  
**24 бита** – адрес сети,  
**8 бит** – хостовая часть

Маска /24 CIDR записывается:  
**1111 1111.1111 1111.1111 1111.0000 0000**  
(24 + 8) или **255.255.255.0**

# Число адресов в подсети легко определить по CIDR

$$2^8 = 256$$

```
vagrant@vagrant:~$ netmask -s 10.0.2.15/24  
10.0.2.0/255.255.255.0
```

# Специальные адреса подсети

1

## Широковещательный адрес сети

пакеты с широковещательным  
адресом получают все хосты этой  
сети

2

## Адрес сети

позволяет определить, что  
хосты находятся в одной сети

# Как вычисляются специальные адреса подсети?

1

Широковещательный  
адрес сети



ADDRESS **OR, NOT** MASK

192.168.0.255

2

Адрес сети



ADDRESS **AND** MASK

192.168.0.0

# Логическое И

**0**

если хотя бы один  
из битов равен **0**

**1**

если оба бита  
равны **1**

# Пример

Результат применения  
логического И – адрес сети

```
    00110 &  
    01011  
=    00010  
>>> res = 0b00110 & 0b01011;  
>>> format(res, '05b')  
'00010'
```

# Логическое ИЛИ

**0**

если оба бита  
равны **0**

**1**

если хотя бы один  
из битов равен **1**



# Пример

Результат применения  
логического ИЛИ

```
00110 &  
11111  
=  
11111  
>>> res = 0b00110 | 0b11111;  
>>> format(res, '05b')  
'11111'
```

# Пример

Результат применения  
логического И между  
инвертированной маской сети и  
адресом хоста – бродкаст адрес

```
00110 &  
11111  
=  
11111  
>>> res = 0b00110 | 0b11111;  
>>> format(res, '05b')  
'11111'
```

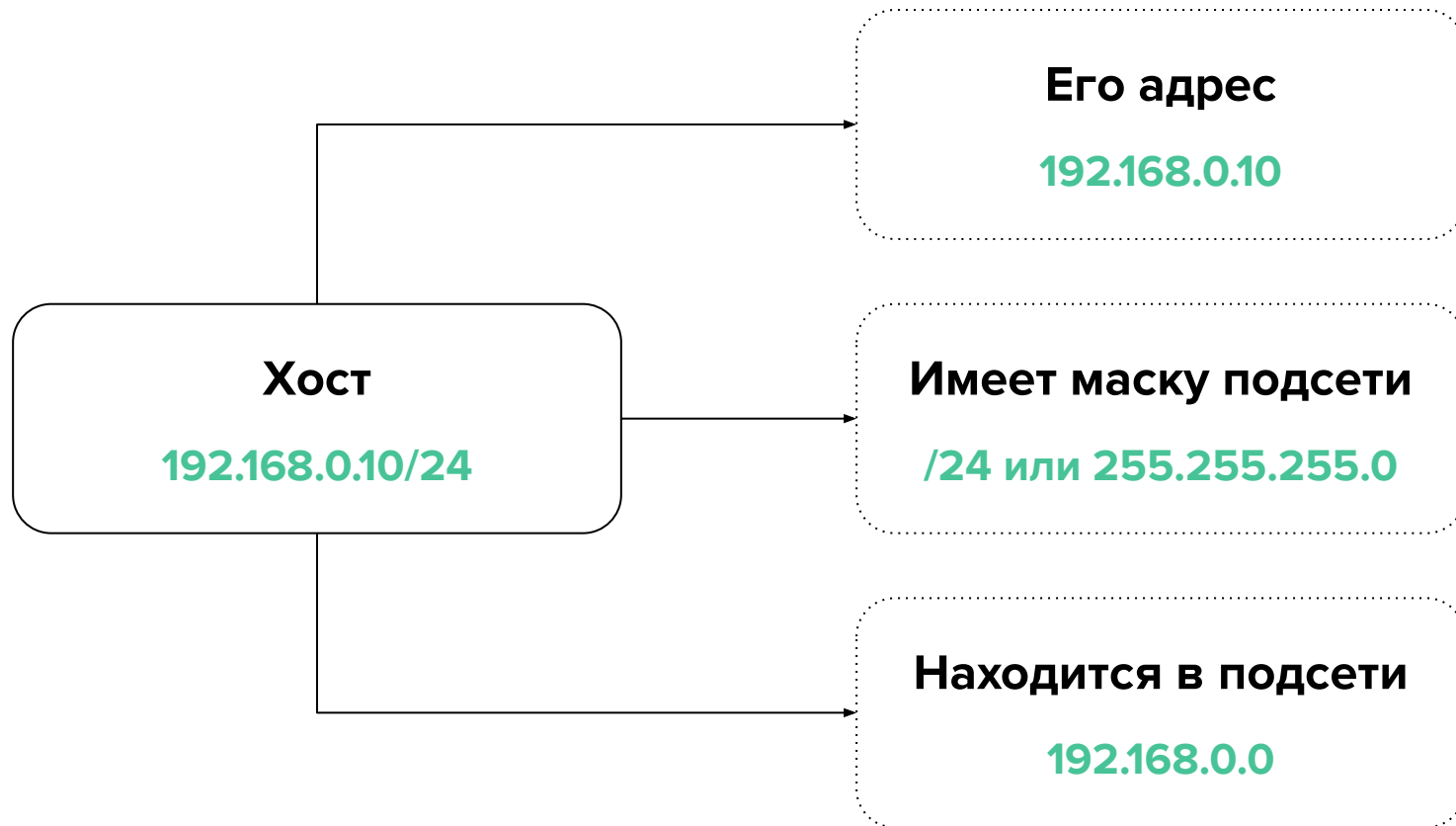
# Рассмотрим IP-адрес 192.168.0.1/24



# Простой пример применения маски IPv4

Сетевая часть (n) / хостовая (h)	nnnnnnnn	nnnnnnnn	nnnnnnnn	hhhhhhh
Адрес десятичный	192	168	0	10
Адрес двоичный	11000000	10101000	00000000	00001010
Маска десятичная	255	255	255	0
Маска двоичная	11111111	11111111	11111111	00000000
Инвертированная маска	00000000	00000000	00000000	11111111
Адрес сети двоичный	11000000	10101000	00000000	00000000
Адрес сети десятичный	192	168	0	0
Бродкаст адрес двоичный	11000000	10101000	00000000	11111111
Бродкаст адрес десятичный	192	168	0	255

# Простой пример применения маски IPv4



**По стандарту маски  
должны обеспечивать  
смежность подсетей, поэтому  
они всегда будут выглядеть  
как последовательность из  
1 в начале и 0 в конце**

# Особенности нумерации IPv4

192.168.0.0

Специальный зарезервированный адрес, который называется **адресом сети**

192.168.0.255

Последний адрес подсети, является зарезервированным, предназначен для **широковещательных сообщений** на уровне L3

192.168.0.1

**Первый доступный адрес сети** – часто адрес шлюза, через который можно попасть в другие сети

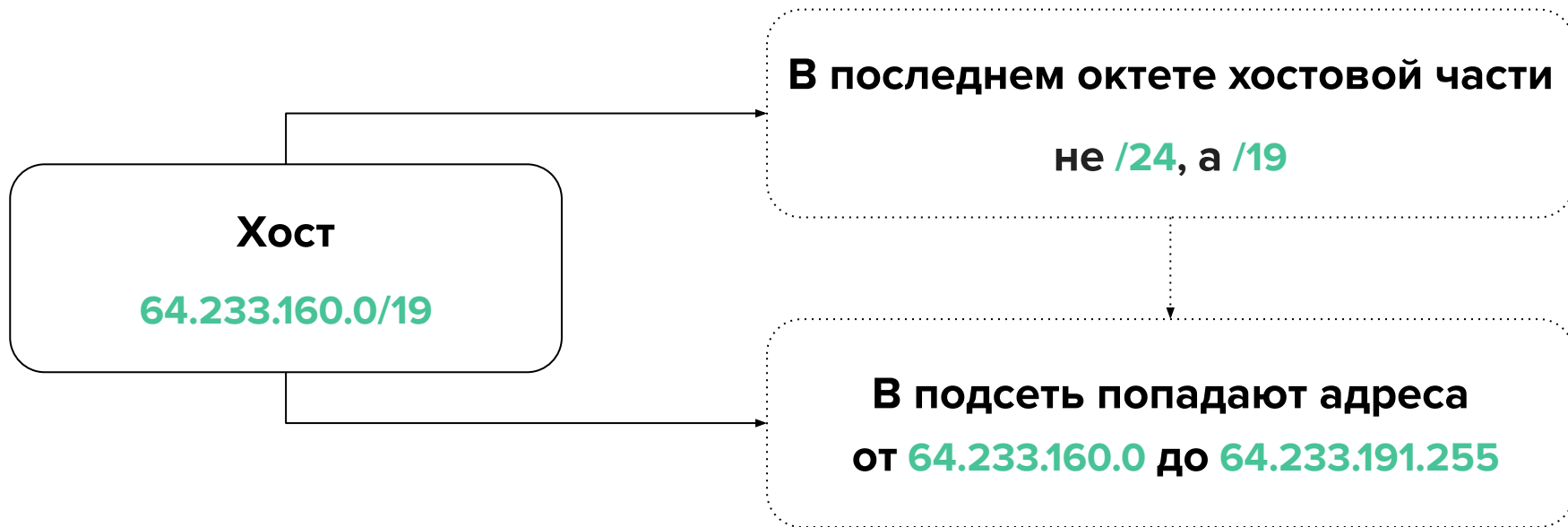
# Сложный пример применения маски IPv4

Маска десятичная	255	255	224	0
Адрес десятичный	64	233	161	138
Адрес двоичный	01000000	11101001	10100001	10001010
Маска двоичная	11111111	11111111	11100000	00000000
Сетевая часть	nnnnnnnn	nnnnnnnn	nnn	
Хостовая часть			hhhhh	hhhhhhh
Адрес сети двоичный	01000000	11101001	10100000	00000000
Адрес сети десятичный	64	233	160	0

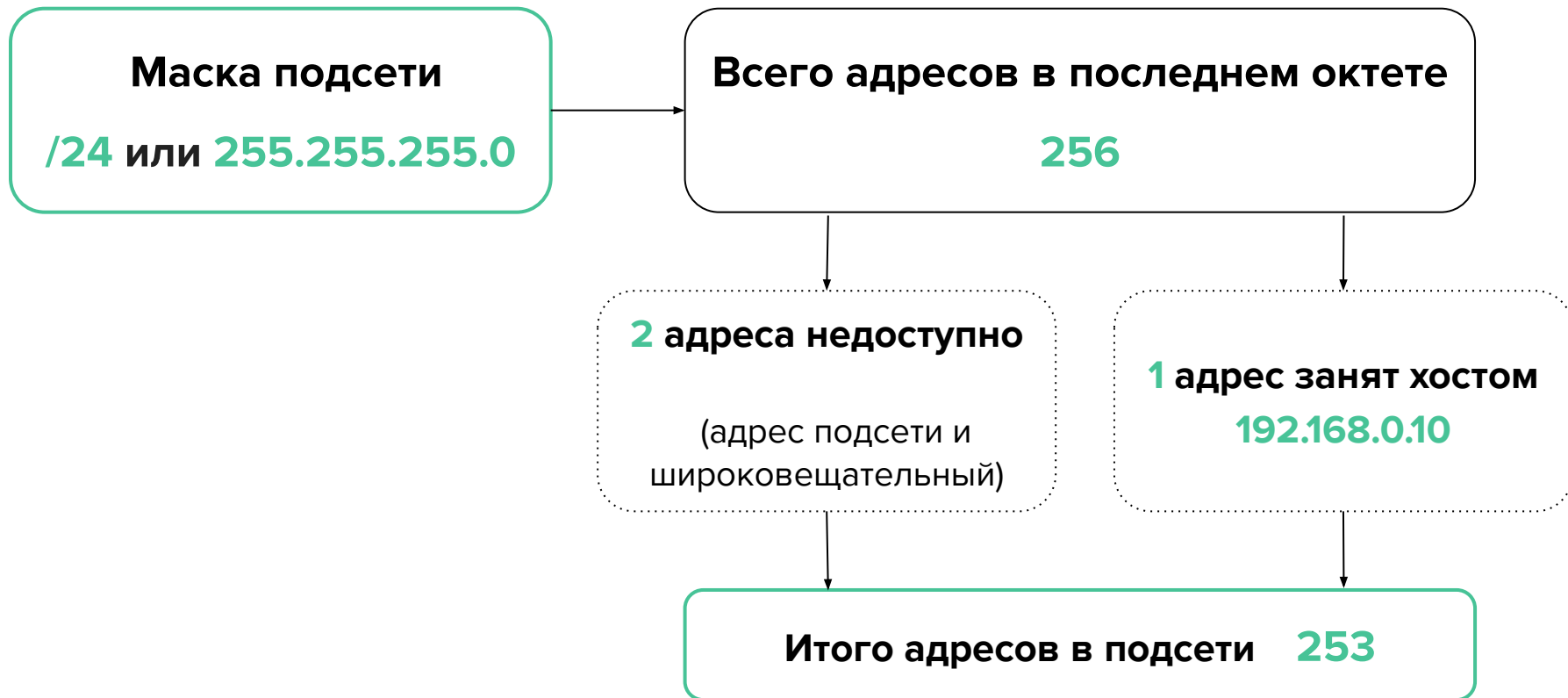


# Сложный пример применения маски IPv4

```
vagrant@vagrant:~$ google_v4_addr=$(dig +short A google.com | head -n1)
vagrant@vagrant:~$ echo $google_v4_addr; whois $google_v4_addr | grep CIDR
64.233.161.138
CIDR:      64.233.160.0/19
```



# Особенности нумерации IPv4



# Автоматизированный калькулятор ipcalc

```
vagrant@vagrant:~$ ipcalc 192.168.0.10/24
```

```
Address: 192.168.0.10      11000000.10101000.00000000. 00001010
```

```
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
```

```
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
```

# Пояснение к примеру



\* $2^8 = 256$  – диапазон адресов от 0 до 255 и минус адрес сети и широковещательный адрес

# Адреса со специальным назначением

**127.0.0.1**

Стандартный адрес  
**loopback** интерфейса из  
огромной (+16 млн.) подсети  
**127.0.0.0/8**

**10.0.0.0/8,**  
**172.16.0.0/12,**  
**192.168.0.0/16**

Немаршрутизируемые  
частные сети

**169.254.0.0/16**

Немаршрутизируемые  
link-local адреса, которые  
назначаются, например,  
при неуспешной работе  
DHCP клиента

**224.0.0.0/4**

Диапазон для **multicast**  
(широковещательная  
групповая передача)

**100.64.0.0/10**

Для **carrier-grade NAT**

И многие другие

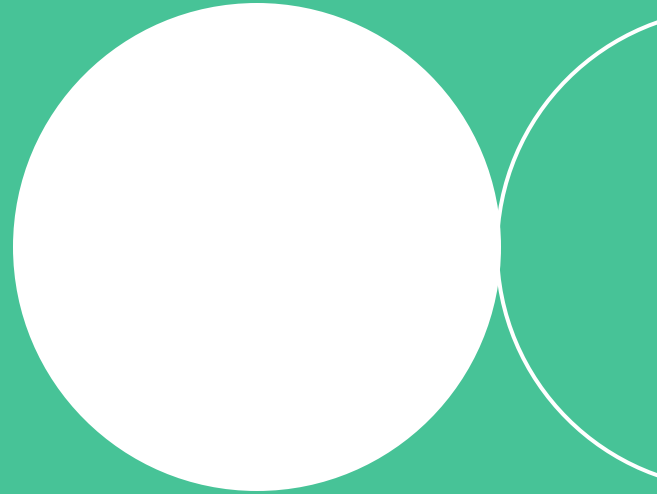
[полный список](#)

# Итоги темы

- 1 В каждой сети должны присутствовать два особых адреса: адрес сети и широковещательный адрес сети, на который будут рассылаться broadcast-запросы
- 2 Маска подсети позволяет вычислять адрес сети, широковещательный адрес. Все адресное пространство между этими адресами будет ёмкостью сегмента
- 3 Существует большое количество специальных диапазонах IP адресов. Для создания локальных сетей используют диапазоны 192.168.0.0/16 172.16.0.0/12 и 10.0.0.0/8 . Для обращения к самому себе – диапазон 127.0.0.0/8

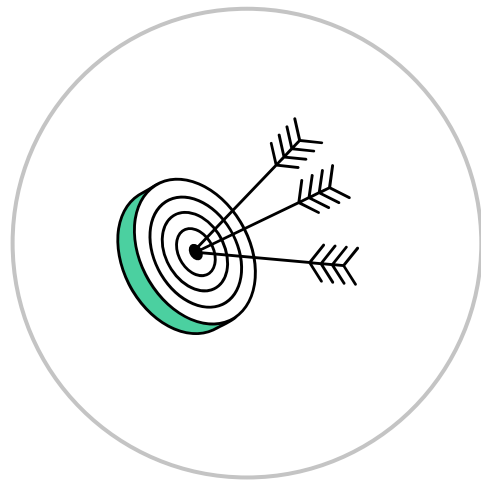


# IPv6



# Цели темы

- Обзорно познакомиться с IPv6
- Узнать о ключевых отличиях IPv6 от IPv4





**Большинство приложений  
работают с IPv6, решены  
проблемы dual-stack систем  
(с IPv4 и IPv6 одновременно)**

# IPv6 утилиты

ping6

tracert6

dual-stack

ip -6

/etc/gai.conf

для настройки

# IPv6

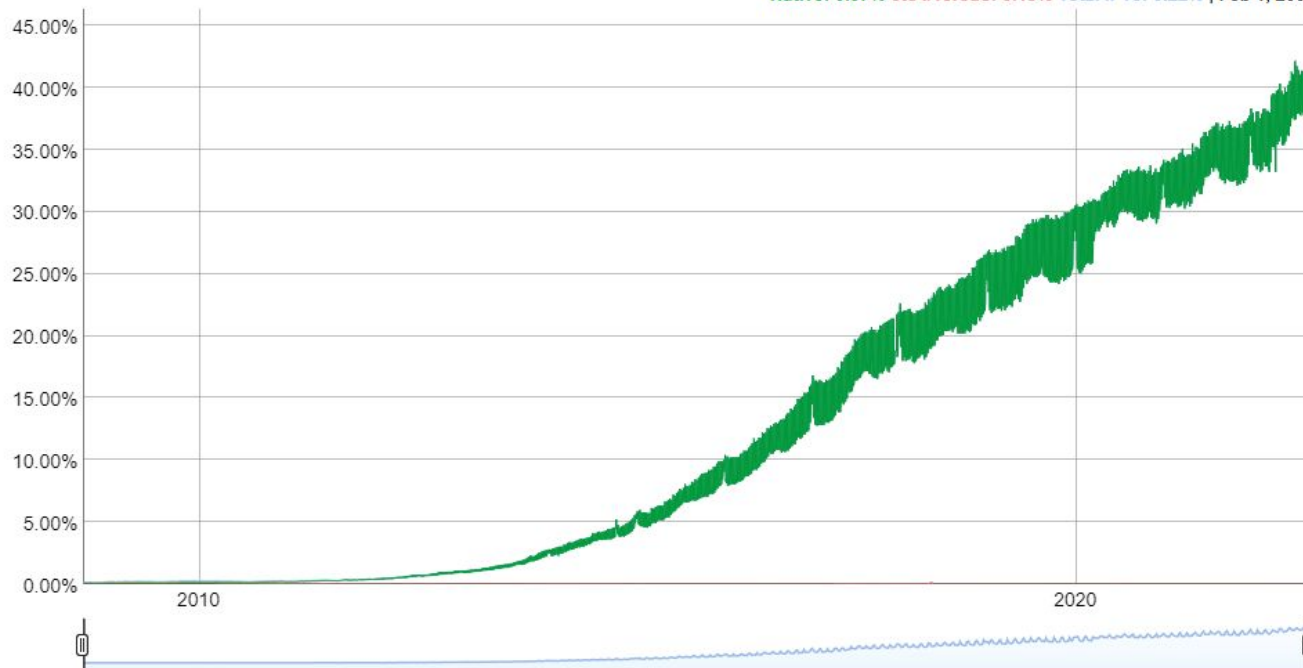
## IPv6 Adoption

### Per-Country IPv6 adoption

## IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

Native: 0.07% 6to4/Teredo: 0.15% Total IPv6: 0.22% | Feb 1, 2009





## IPv6

**новый стандарт протокола IP,  
призванный исправить недостатки IPv4**



# Преимущества IPv6

- Увеличенное адресное пространство (128 бит)
- Автоконфигурация (не нужно настраивать адреса вручную)
- Jumbogram (передача до 4 Гб данных в одном пакете)

# IPv6 имеет вид

**2001:0:0:0:DB8:800:200C:417A**

Полный формат

**2001::DB8:800:200C:417A**

Сокращенный формат

**https://[2001:0:0:0:DB8:800:200C:417A]:8080/**

При использовании в URL, необходимо заключать в скобки [ ]

# IPv6 трафик может быть:



Unicast

Обычный трафик  
хоста

Anycast

Групповой трафик,  
пакет будет доставлен  
наиболее близкому  
хосту с точки зрения  
протокола  
маршрутизации

Multicast

Групповой трафик,  
пакеты будут  
доставлены каждому  
хосту в группе

Broadcast

Не реализован

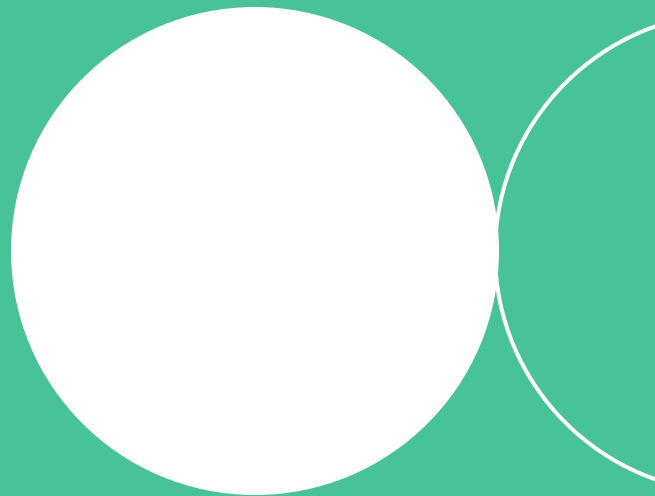
# Итоги темы

- 1 IPv6 является “работой над ошибками”, выявленными при использовании IPv4: увеличенное адресное пространство, передача Jumbogram, автоконфигурация адресации
- 2 IPv6 активно распространяется и рано или поздно полностью вытеснит IPv4
- 3 В IPv6 отказались от широковещательных сообщений, но добавили новый тип трафика - anycast, к ближайшему с точки зрения адресации узлу



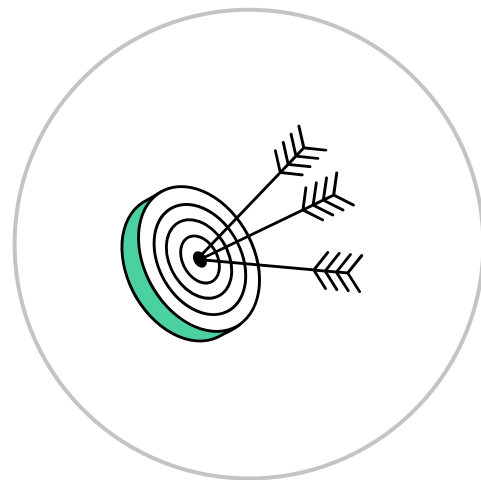


# Работа маршрутизатора



# Цели темы

- Познакомиться с концепцией маршрутов и задачей маршрутизатора
- Понять ключевые отличия маршрутизации L3 от L2





**Как происходит  
взаимодействие устройств  
в разных сетях?**

# Задача маршрутизатора

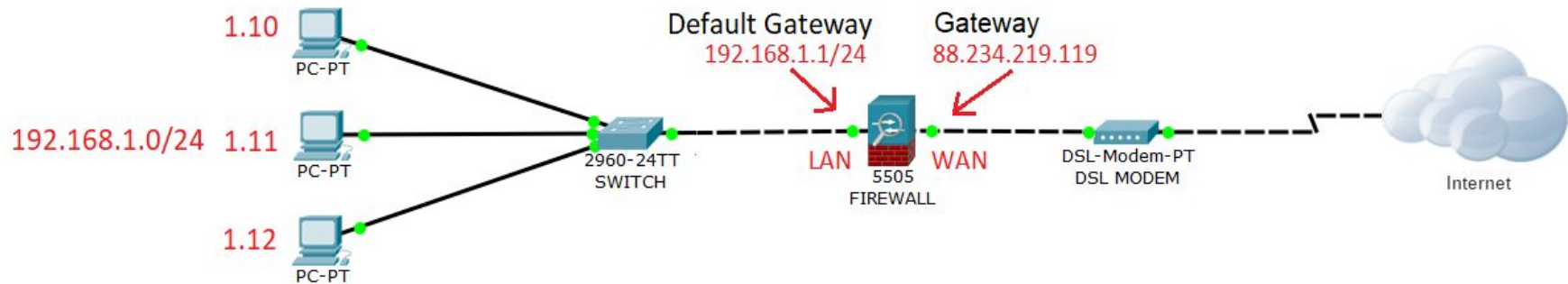
**объединение сетей  
на сетевом уровне**

# Маршрутизатор

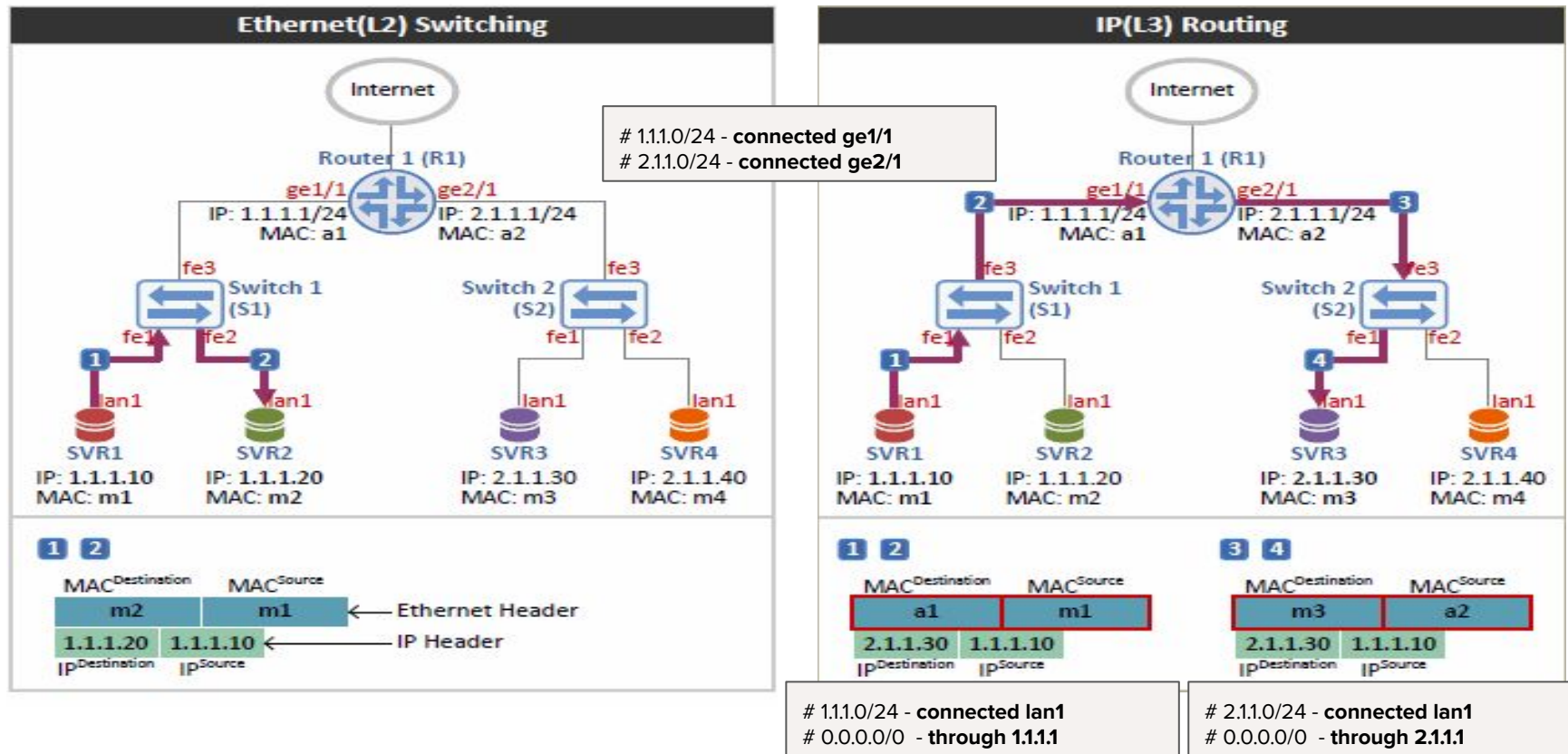


**При работе маршрутизатор  
вынужден подменять MAC-  
адрес запроса на свой  
собственный MAC-адрес  
в другом сегменте**  
(он объединяет несколько  
сегментов – это его задача)

# Маршрут по умолчанию (default gateway)



# Двухуровневая адресация





# Итоги темы

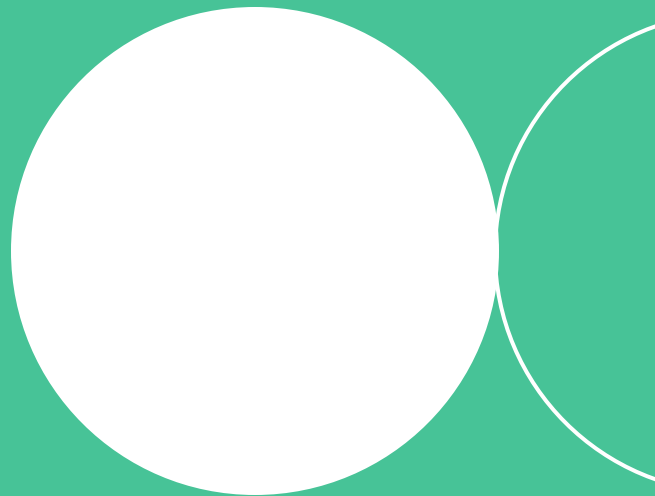
- 1 Шлюз по умолчанию или default gateway – узел в сети, на который IP пакет отправляется, если маршрут к сети назначения неизвестен
- 2 Маршрутизатор, находясь на границе двух и более сегментов сети, объединяет их, связывая воедино
- 3 Для пересылки пакета из одного сегмента в другой маршрутизатор осуществляет подмену MAC адреса в кадре для доставки его адресату
- 4 Взаимодействие на уровне L2 проходит без какого-либо участия маршрутизатора



**Перерыв**

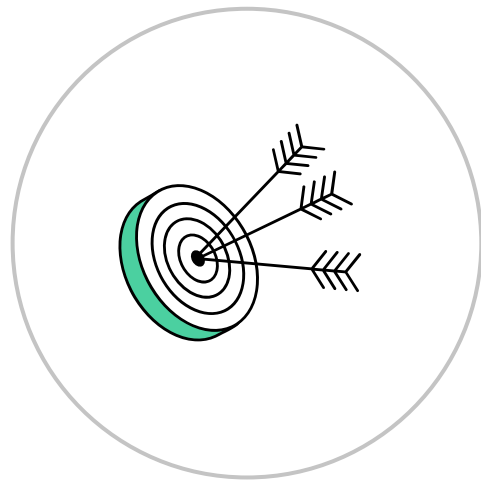


# Маршрутизация



# Цели темы

- Узнать о видах маршрутизации
- Получить представление о статической маршрутизации, практических инструментах по составлению таблицы маршрутизации
- Познакомиться с общим принципом работы динамической маршрутизации, видами реализующих ее протоколов






## Статическая маршрутизация

**вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора**



The background features three large, light gray circles that overlap each other. The central circle is the most prominent, and the text is centered within it. The other two circles are partially visible on the left and right sides of the frame.

**Вся маршрутизация при этом  
происходит без участия каких-  
либо протоколов  
маршрутизации**



## Динамическая маршрутизация

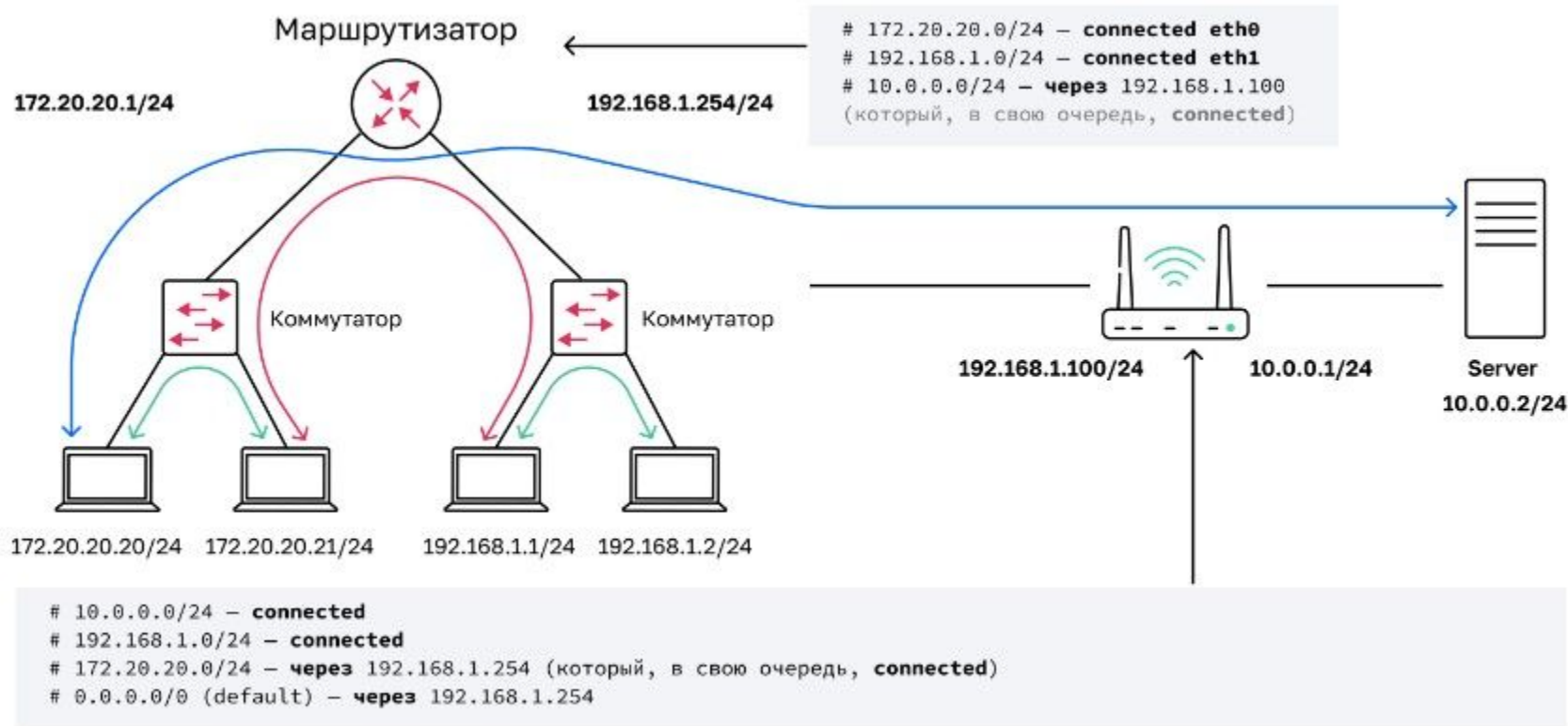
вид маршрутизации, при котором таблица маршрутизации редактируется программно



**Вы настраиваете **протокол  
маршрутизации**, а он вносит  
изменения в таблицу  
маршрутизации**



# Статическая маршрутизация



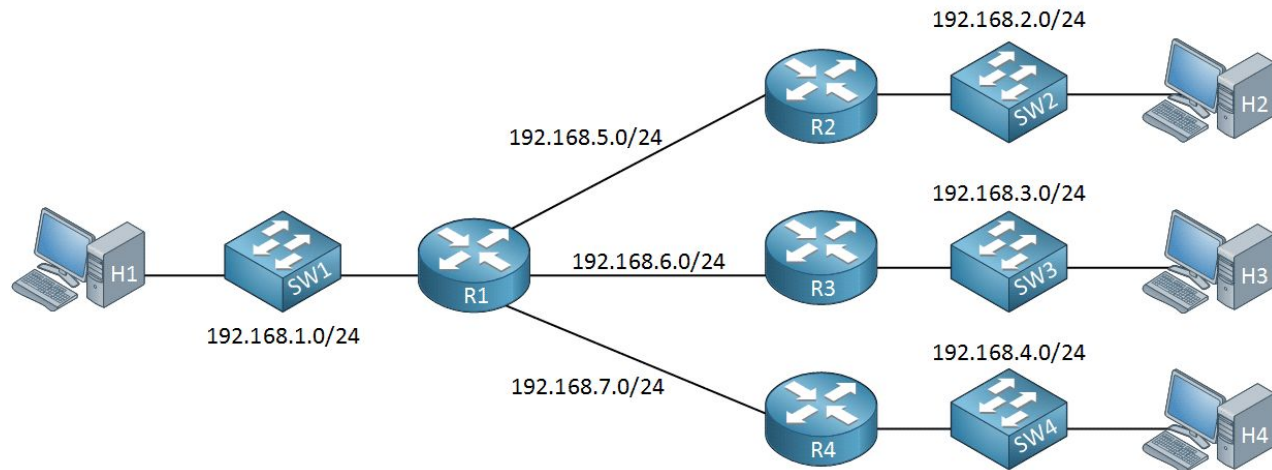
# Динамическая маршрутизация

192.168.1.0/24 – R1

192.168.2.0/24 – R2

192.168.3.0/24 – R3

192.168.4.0/24 – R4



# Протоколы маршрутизации делятся по типу алгоритмов

Дистанционно-векторные  
протоколы  
Distance Vector

**RIP**

(зависит от количества хопов)

Протоколы состояния  
каналов  
Link-state

**OSPF**

(зависит от метрик линков)

Усовершенствованные  
дистанционно-векторные  
Distance Vector

**EIGRP**

(смесь)

# Протоколы маршрутизации делятся по области применения

**Междоменная  
маршрутизация**

**BGP**

**Внутридоменная  
маршрутизация**

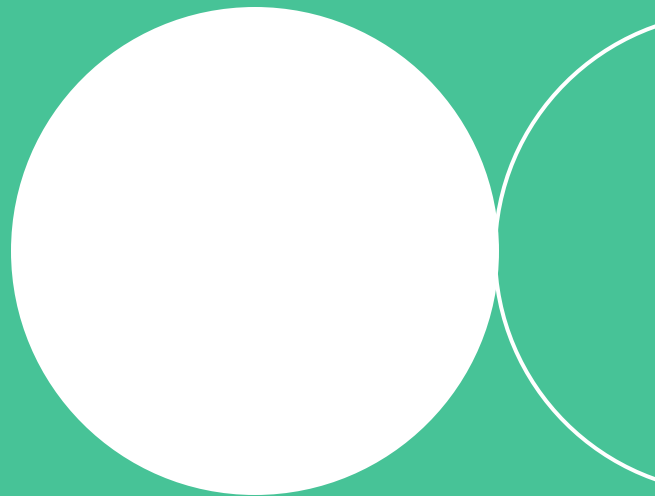
**OSPF, RIP, EIGRP**

# Итоги темы

- 1 Маршрутизация бывает статической и динамической
- 2 При относительно небольшом количестве сегментов сети и постоянстве их конфигурации целесообразно использовать статические маршруты
- 3 Если сеть включает большое количество сегментов и топология часто меняется необходимо использовать динамическую маршрутизацию
- 4 Протоколы динамической маршрутизации делятся на внешние/внутренние или по типу алгоритма. Сетевое оборудование непосредственно влияет на выбор того или иного протокола

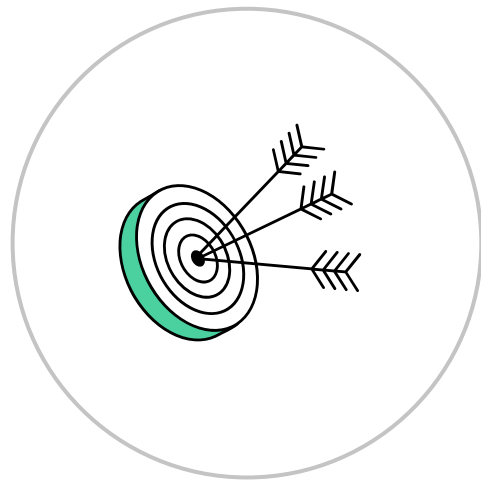


# Популярные сетевые утилиты



# Цели темы

- Познакомиться с популярными утилитами для диагностики L3
- Получить практические навыки поиска и устранения проблем связанных с неправильной настройкой на уровне L3



# Дословный перевод TTL

Time To Live



Время жизни





## TTL

**время жизни пакета данных в протоколе IP (предельно допустимое время его пребывания в системе)**



# При прохождении IP пакета через роутер

Роутер  
уменьшает TTL  
на единицу

Пакеты, в  
которых TTL  
достиг нуля,  
уничтожаются

Роутер  
формирует  
сообщение  
ICMP Time  
Exceeded

# Данное свойство используется в traceroute:

Формируется пакет с **TTL = 1**, первый на пути следования роутер уменьшает TTL до 0 и отвечает **Time Exceeded** (первый хоп)

Traceroute формирует пакет с **TTL = 2**, он успешно преодолевает первый роутер, и уже второй отвечает **Time Exceeded**

Когда traceroute вместе **Time Exceeded** получает **Connection Refused** или случайно выбранный порт совпадает с каким-то слушающим сервисом, искомый хост считается достигнутым



**Используя `src IP` и метки  
времени, `tracert` узнает  
трассу прохождения пакета и  
время его прохождения**

# Traceroute в Linux использует:

По умолчанию  
**UDP** пакеты со  
случайным портом

Можно выбрать  
ключи **TCP (-T)** или  
**ICMP** режим **(-I)**

Утилита **mtr**  
собирает статистику

# MAC и IP

## Интерфейсы

```
osboxes@osboxes:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT
group default qlen 1000
    link/ether 08:00:27:f4:39:50 brd ff:ff:ff:ff:ff:ff
```

## Адреса для IPv4

```
osboxes@osboxes:~$ ip -4 address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
1000
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86328sec preferred_lft 86328sec
```

# Ping

## Ping (ICMP echo request + ICMP echo reply)

```
osboxes@osboxes:~$ ping -c 1 netology.ru
PING netology.ru (104.26.8.143) 56(84) bytes of data.
64 bytes from 104.26.8.143 (104.26.8.143): icmp_seq=1 ttl=63 time=3.88 ms
--- netology.ru ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.877/3.877/3.877/0.000 ms
```

# Ping

Попробуем что-то поинтереснее:

```
osboxes@osboxes:~$ ping -M do -s $((2000-28)) -c1 netology.ru
```

```
PING netology.ru (172.67.75.22) 1972(2000) bytes of data.
```

```
ping: local error: message too long, mtu=1500
```

```
--- netology.ru ping statistics ---
```

```
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

```
osboxes@osboxes:~$ ping -M do -s $((1500-28)) -c1 netology.ru
```

```
PING netology.ru (172.67.75.22) 1472(1500) bytes of data.
```

```
1480 bytes from 172.67.75.22 (172.67.75.22): icmp_seq=1 ttl=63 time=10.1 ms
```

```
--- netology.ru ping statistics ---
```

```
1 packets transmitted, 1 received, 0% packet loss, time 0ms
```

```
rtt min/avg/max/mdev = 10.135/10.135/10.135/0.000 ms
```

Где 28 –

длина заголовков IP (20) + ICMP (8)



# Как tcpdump поможет при проблемах с маской?

```
root@netology1:~# ip -4 a s eth1 | grep inet
inet 172.28.128.10/24 scope global eth1
root@netology2:~# ip -4 a s eth1 | grep inet
inet 172.28.128.60/24 scope global eth1
root@netology1:~# ip r get 172.28.128.60
172.28.128.60 dev eth1 src 172.28.128.10 uid 0
```

**curl 172.28.128.60** работает

Ломаем на хосте **netology2** сеть, устанавливая заведомо некорректную маску:

```
root@netology2:~# ip addr del 172.28.128.60/24 dev eth1
root@netology2:~# ip addr add 172.28.128.60/30 dev eth1 # вместо /24
root@netology2:~# ip -4 a s eth1 | grep inet
inet 172.28.128.60/30 scope global eth1
```

# Как tcpdump поможет при проблемах с маской?

Если запустить в этот момент **tcpdump** на обоих хостах, будет видно, что **SYN** доходит до сервера, но он не отвечает клиенту **SYN+ACK**, и клиент перепосылает **SYN**:

```
root@netology1:~# tcpdump -nn -i eth1
10:34:38.393610 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
10:34:39.423744 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
root@netology2:~# tcpdump -nn -i eth1
10:34:37.621593 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
10:34:38.652240 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
```

Это только один из примеров, как **tcpdump** быстро покажет, на каком хосте случились проблемы с сетью. Зная, как устанавливается TCP соединение, можно увидеть, на какой стадии происходит проблема и на каком хосте

# Практика



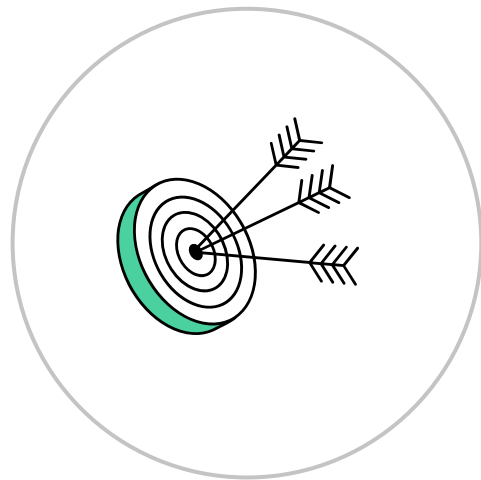
# Итоги темы

- 1 Для получения информации о маршруте существуют различные утилиты использующие поле TTL в заголовке IP-пакета. Самые популярные это traceroute и mtr
- 2 Доступность удаленного узла на уровне L3 поможет определить утилита ping
- 3 Одной из лучших утилит для диагностики на всех уровнях является tcpdump. Благодаря ей и знанию метаданных можно отследить причину возникновения тех или иных сбоев



# Общие итоги занятия

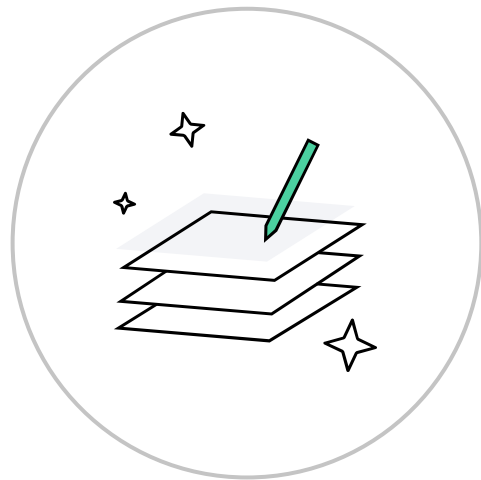
- Разобрали основы работы сетевого уровня модели OSI
- Изучили протокол IPv4: возможности, ограничения и особенности адресации
- Познакомились с протоколом IPv6 и поняли его ключевые отличия от IPv4
- Поняли особенности маршрутизации в сетях на уровне L3 на примере работы роутера
- Научились строить статический и динамический маршруты
- Научились работать с сетевыми утилитами для диагностики и настройки сетей на уровне L3



# Домашнее задание

## Давайте посмотрим вашу практику после лекции

- 1 Практика состоит из обязательного теста и домашнего задания со звездочкой (необязательное)
- 2 В тесте 14 вопросов, на 10 нужно ответить верно. Есть 2 попытки
- 3 Вопросы по домашнему заданию со звездочкой задавайте в чате группы
- 4 Задачи можно сдавать по частям.  
Зачёт по домашней работе ставят после того, как приняты все задачи



# Задавайте вопросы. Оставляйте обратную связь по вебинару

Ильмир Сахипов  
Руководитель центра управления сетью АО “Уфанет”

