Протокол IP

Структура, CIDR, NAT.

09-431
Зараменских Ульяна
Тихонова Елизавета

Что такое стек протоколов

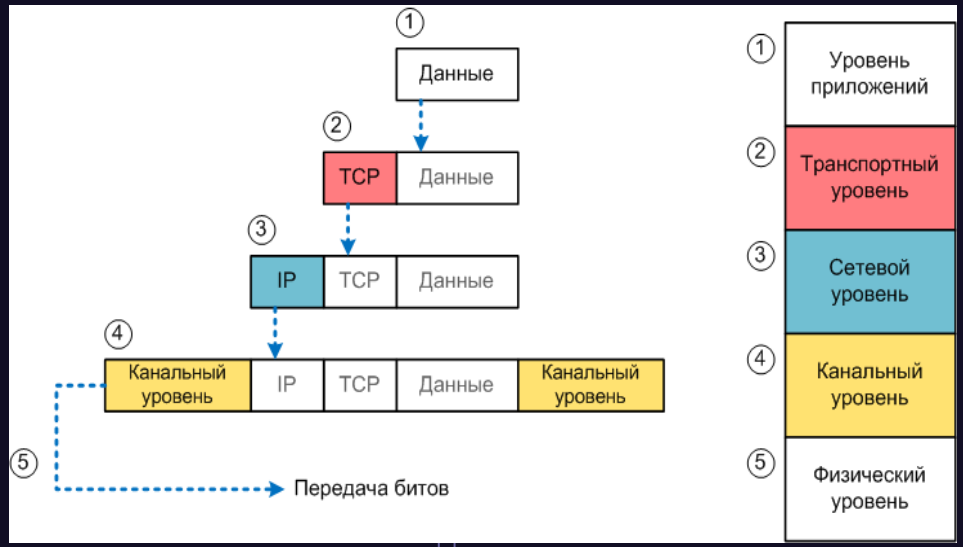
Стек протоколов – иерархически организованный набор протоколов, работающих совместно для передачи данных.

Принцип работы:

- Каждый уровень решает свою задачу
- Уровень предоставляет сервис верхнему уровню
- Уровень не зависит от внутреннего устройства нижнего

Декапсуляция – обратный процесс на принимающей стороне.

Инкапсуляция :



История: OSI vs TCP/IP

OSI/ISO (1980-е):

- Разработан международной организацией ISO
- 7 уровней
- Теоретический эталон, академический подход
- Внедрение затянулось из-за согласований

TCP/IP (1970-е):

- Разработан для ARPANET (DARPA, США)
- 4 уровня
- Практическая реализация, работал «здесь и сейчас»
- Стал стандартом де-факто

Итог: практика победила теорию.

Сравнение уровней OSI и TCP/IP

OSI (7 уровней)	TCP/IP (4 уровня)
7. Прикладной 6. Представления 5. Сеансовый	Прикладной
4. Транспортный	Транспортный
3. Сетевой	Межсетевой
2. Канальный 1. Физический	Доступ к сети

Протокол IP

Протокол IP: общая характеристика

IP (Internet Protocol) – межсетевой протокол.

Ключевая характеристика: Best Effort («максимальные усилия»)

Что НЕ делает IP:
- Не устанавливает соединение (connectionless)
- Не гарантирует доставку пакетов
- Не гарантирует порядок доставки
- Не гарантирует целостность данных

Что делает IP:
- Адресация устройств
- Маршрутизация пакетов между сетями
- Фрагментация пакетов при необходимости

Надежность – задача верхних уровней (TCP).

Структура IP-адреса

Ipv4 в десятиричном виде



Классы сетей IP

класс сети	диапазон значений первого разряда (байта)	наименьший номер сети	наибольший номер сети	максимально возможное количество сетей в классе	максимально возможное количество узлов в сети класса
A	1-126	1.0.0.0	126.0.0.0	126	16 777 214
B	128-191	128.0.0.0	191.255.0.0	16 382	65 534
C	192-223	192.0.0.0	223.255.255.0	2 097 150	254
D	224-239	224.0.0.0	239.255.255.255	групповые адреса + резерв	
E	240-247	240.0.0.0	247.255.255.255	зарезервировано	
сеть 127.0.0.0 – используется для самопроверки и самодиагностики					
нули в номерах сетей – для хостов (максимальное их число в каждом разряде - 254)					

Проблема классовой модели:

- Жесткость: нужно 300 адресов → выдается класс B (65 000 адресов)
- 64 700 адресов пропадают зря
- Неэффективное использование адресного пространства

Виды трафика



Unicast (один к одному)

- Стандартный обмен данными
- Пример: запрос веб-страницы



Multicast (один к группе)

- Вещание для подписчиков группы
- Пример: IP-TV, видеоконференции



Broadcast (один ко всем)

- Рассылка всем устройствам в локальной сети
- Пример: ARP-запрос, DHCP Discover
- Не выходит за пределы локальной сети



Anycast (один к ближайшему)

- Пакет уходит к ближайшему из группы серверов
- Пример: DNS-серверы 8.8.8.8

Специальные адреса

Loopback: 127.0.0.1
- Адрес «самого себя» (localhost)
- Используется для проверки стека TCP/IP

Broadcast: 255.255.255.255
- Рассылка всем устройствам в сети

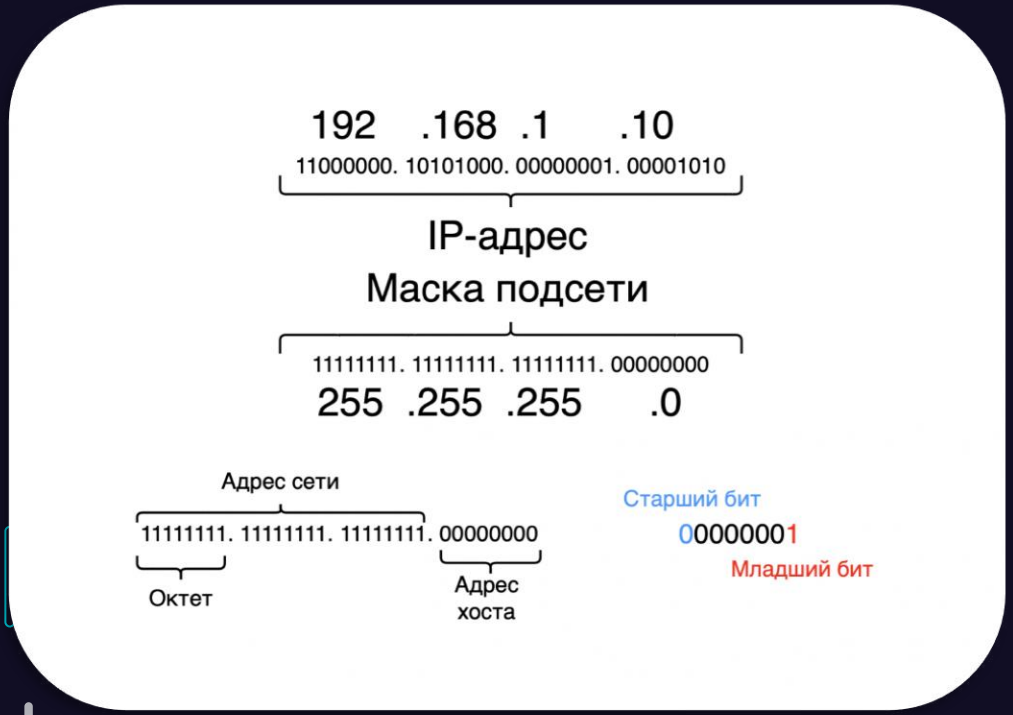
Частные (серые) адреса — не маршрутизируются в интернете:
- 10.0.0.0/8 (большие корпоративные сети)
- 172.16.0.0/12 (средние сети)
- 192.168.0.0/16 (домашние сети, ваш роутер)

Для выхода в интернет частный адрес заменяется на публичный через NAT.

Формат пакета IP

<table>
<tr><td>Версия
(Version)</td><td>Длина
(IHL)</td><td>Тип сервиса
(ToS)</td><td colspan="2">Общая длина пакета
(Total Lenght)</td></tr>
<tr><td colspan="3">Идентификатор</td><td>Флаги</td><td>Смещение фрагмента</td></tr>
<tr><td>Время жизни
(TTL)</td><td colspan="2">Протокол
(см. след. слайд)</td><td colspan="2">Контрольная сумма</td></tr>
<tr><td colspan="5">Адрес отправителя
(Source IP address)</td></tr>
<tr><td colspan="5">Адрес получателя
(Destination IP address)</td></tr>
<tr><td colspan="4">Опции (поле переменной длины)</td><td>Выравнивание до 32 бит
(padding)</td></tr>
</table>

Маски подсети: введение



Правило:

- Единицы в маске = биты адреса сети
- Нули в маске = биты адресов хостов

Операция AND (логическое И):

IP AND Маска = адрес сети

192.168.1.10 AND 255.255.255.0 = 192.168.1.0

Маска всегда состоит из сплошных единиц, за которыми идут нули.

255.0.255.0 — некорректная маска.

Организация подсетей: зачем делить сеть

Организация подсетей (сабнеттинг) - разделение одной большой сети на несколько меньших логических подсетей.

Зачем это нужно:

- Безопасность: изолировать отделы друг от друга
- Производительность: уменьшить broadcast-домен
- Управляемость: проще администрировать
- Экономия адресов: не тратить целую сеть /24 на 10 компьютеров

Пример:

Компания получила сеть 192.168.1.0/24 (254 хоста).
Нужно разделить на:

- Отдел продаж -50 компьютеров
- Бухгалтерия - 20 компьютеров
- Серверная - 10 компьютеров
- Гостевая Wi-Fi - 30 устройств

Решение: разбить /24 на несколько подсетей с помощью масок.

Организация подсетей: практический пример

Задача: разбить 192.168.1.0/24 на 4 подсети.

Исходная сеть: /24 = 256 адресов, 254 хоста.
Нужно 4 подсети → занимаем 2 бита у хостов (2^2 = 4).

Новая маска: /24 + 2 = /26 (255.255.255.192)
Каждая подсеть: 2^(32-26) = 64 адреса, 62 хоста.

Результат:

Подсеть	Диапазон	Broadcast	Хосты
192.168.1.0/26	.0 – .63	.63	.1 – .62
192.168.1.64/26	.64 – .127	.127	.65 – .126
192.168.1.192/26	.128 – .191	.191	.129 – .190
192.168.1.192/26	.192 – .255	.255	.193 – .254

Правило: чтобы получить N подсетей, нужно занять $\log_2$ (N) бит у хостов.

CIDR

CIDR: что это и зачем

CIDR (Classless Inter-Domain Routing) - бесклассовая маршрутизация.
Введена в 1993 году для борьбы с нехваткой IPv4-адресов.

Формат записи: IP-адрес / количество бит маски
Пример: 192.168.1.0/24 = 192.168.1.0 с маской 255.255.255.0

/24 означает: 24 бита отведено под адрес сети, 8 бит — под хосты.

Преимущества CIDR:

- Экономия адресного пространства (выдача ровно столько, сколько нужно)
- Гибкость (маски любой длины)
- Агрегация маршрутов (суммирование сетей)
- Замена жесткой классовой модели

CIDR: формула расчета

Соответствие префиксов CIDR, десятичных масок и количества хостов

Префикс	Количество бит сети	Количество бит хостов	Десятичная маска	Количество хостов
/24	24	8	255.255.255.0	254
/25	25	7	255.255.255.128	126
/26	26	6	255.255.255.192	62
/27	27	5	255.255.255.224	30
/28	28	4	255.255.255.240	14
/29	29	3	255.255.255.248	6
/30	30	2	255.255.255.252	2

Формула:

Количество хостов = $2^{32} - 2$

Где:

32 – длина маски

вычитаемые 2 – это адрес сети и широковещательный адрес.

CIDR: практический пример

Задача: дан адрес 10.0.0.50 с маской /28.
Найти: адрес сети, broadcast, диапазон хостов, маску в десятичном виде.

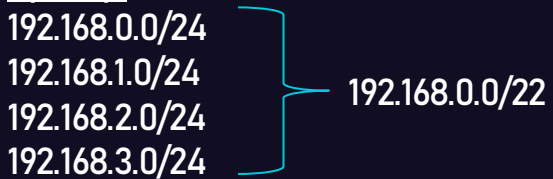
Решение:

1. Биты хостов: 32 − 28 = 4
2. Всего адресов: 2^4 = 16
3. Блоки подсетей идут по 16: ...32 | 48 | 64...
   Наш адрес 50 попадает в блок 48–63.
4. Адрес сети: 10.0.0.48
5. Broadcast: 10.0.0.63
6. Хосты: 10.0.0.49 – 10.0.0.62 (всего 14)
7. Маска в десятичном виде:
   28 единиц = 24 единицы (255.255.255) + 4 единицы
   4 единицы = 128+64+32+16 = 240
   Маска = 255.255.255.240

CIDR: агрегация маршрутов

Агрегация (суммирование, супернеттинг) — объединение нескольких сетей в одну.

Пример:



Почему /22? Потому что 24 − 2 = 22 (объединили 4 = 2^2 сети).

Зачем нужно:

- Меньше записей в таблице маршрутизации
- Быстрее обработка трафика роутерами
- Критически важно для магистральных сетей (миллионы маршрутов)

Без CIDR современный интернет не справлялся бы с объемом маршрутов.

Отображение MAC-адресов на IP. Протокол ARP и RARP

ARP (Address Resolution Protocol) — сопоставление IP → MAC.

Как работает:

1. Если узлу нужен MAC-адрес получателя, он отправляет широковещательный ARP-запрос (Broadcast): «У кого IP-адрес 192.168.1.10?»
2. Узел-владелец этого IP отвечает одноадресно (Unicast), указывая свой MAC-адрес.
3. Полученная связка IP-MAC сохраняется в локальной таблице.

Таблица соответствия (ARP-кэш):

IP-адрес	MAC-адрес	Тип
192.168.1.1	00:1A:2B:3C:4D:5E	dynamic
192.168.1.10	AA:BB:CC:DD:EE:FF	dynamic

Кэширование: записи хранятся 2–20 минут (зависит от ОС), затем удаляются.
RARP (Reverse ARP): обратный протокол MAC → IP (устарел, заменен DHCP).

Автоматизация назначения IP. Протокол DHCP

DHCP (Dynamic Host Configuration Protocol) - автоматическая выдача IP.

Алгоритм DORA:

1. DHCP Discover (клиент → Broadcast, ищет сервер)
2. DHCP Offer (сервер → клиент, предлагает IP)
3. DHCP Request (клиент → Broadcast, запрашивает IP)
4. DHCP Ack (сервер → клиент, подтверждает аренду)

Структура DHCP-пакета:

0-7 биты	8-15 биты	16-24 биты	25-31 биты
Op (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4 байта)			
Секунды (2 байта)		Флаги (2 байта)	
Ciaddr (4 байта)			
Yiaddr (4 байта)			
Siaddr (4 байта)			
Giaddr (4 байта)			
Chaddr (16 байтов)			
Имя сервера (32 байта)			
Имя загрузочного файла (64 байта)			
Область, зависящая от производителя (32 байта)			
Структура сообщения DHCP			

Протокол IPv6 (Особенности и схема адресации)

IPv6 — протокол следующего поколения.

Основные особенности:
- 128 бит (вместо 32) — неисчерпаемое пространство
- Нет broadcast (только multicast и anycast)
- Встроенный IPSec
- Автоконфигурация (SLAAC)
- Упрощенный заголовок

Типы адресов:
- Unicast (один)
- Multicast (группа)
- Anycast (ближайший)

Схема адресации:
Запись: 8 групп по 16 бит (4 hex-цифры), разделены двоеточием.
2001:0db8:85a3:0000:0000:8a2e:0370:7334

Сокращение:
- Ведущие нули в группе можно опускать: 0db8 → db8
- Группы из нулей можно заменить на «::» (только один раз)

2001:db8:85a3::8a2e:370:7334

Протокол IPv6

Байт	Бит	0		1	2	3
		0-3	4-11	12-15	16-23	24-31
0	0	Версия	Класс трафика	Метка потока		
4	32	Длина полезной нагрузки			След. заголовок	Hop Limit
8-20	64-160	IP-адрес отправителя				
24-36	192-288	IP-адрес получателя				
37-...	320-...	Расширенные заголовки				
...	....	Данные				

Отличия от IPv4:

- Нет контрольной суммы (checksum) — быстрее обработка
- Нет фрагментации на роутерах (только на отправителе)
- Next Header вместо Protocol
- Hop Limit вместо TTL
- Фиксированный размер основного заголовка — 40 байт

Утилиты командной строки

Windows:
ipconfig /all — полная информация о сетевых интерфейсах

Linux:
ip a — современная утилита
ifconfig — устаревшая, но встречается

```
Connection-specific DNS Suffix  . : mydomain.local
Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapte

Physical Address. . . . . . . . . : 08-00-27-37-6F-62
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.215.80(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Sunday, April 2, 2023 1:28:14 PM
Lease Expires . . . . . . . . . . : Monday, April 10, 2023 1:28:14 PM
Default Gateway . . . . . . . . . : 192.168.215.1
DHCP Server . . . . . . . . . . . : 192.168.215.20
DNS Servers . . . . . . . . . . . : 192.168.215.20
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Что смотрим в выводе:
- IPv4-адрес устройства
- Маску подсети
- Шлюз по умолчанию ← это адрес роутера (он делает NAT)
- DNS-серверы

Если шлюз не указан — выхода в интернет не будет, даже если IP есть.

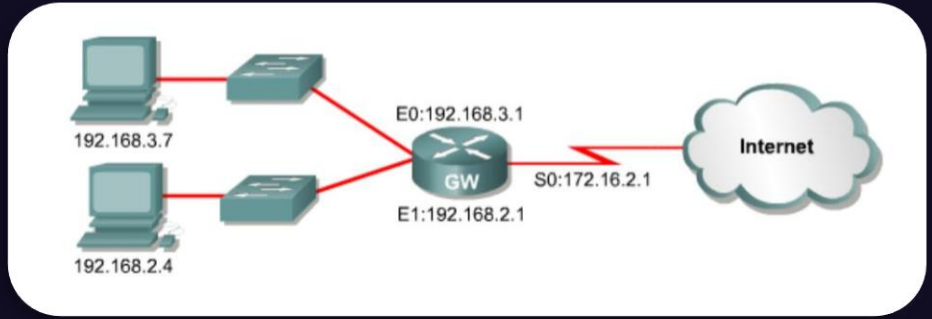
NAT

Система NAT: проблема нехватки адресов и суть технологии

Проблема:
- IPv4-адресов всего ~4.3 млрд
- Устройств в мире — десятки миллиардов
- Публичные адреса закончились еще в 2011 году

NAT (Network Address Translation) — трансляция сетевых адресов. Технология, позволяющая устройствам с частными (серыми) адресами выходить в интернет через один или несколько публичных IP.

Схема:
Локальная сеть (192.168.x.x) → Роутер (NAT) → Публичный IP → Интернет



Система NAT: статический и динамический NAT

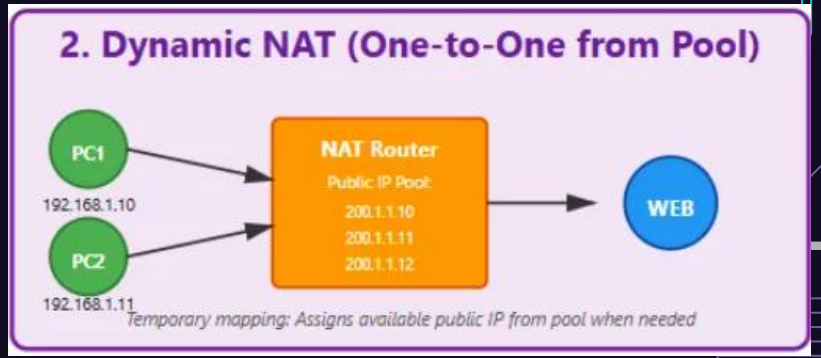
Статический NAT (Static NAT):

- Один внутренний IP ↔ один внешний IP (1:1)
- Жесткая привязка, не меняется
- Используется для серверов, к которым нужен доступ снаружи
- Пример: 192.168.1.10 ↔ 85.140.10.5



Динамический NAT (Dynamic NAT):

- Пул внутренних IP ↔ пул внешних IP
- Адреса выдаются по мере необходимости
- Когда сессия закрывается — адрес возвращается в пул
- Используется в корпоративных сетях



Система NAT:
PAT (NAT Overload) - механизм работы

PAT (Port Address Translation) — NAT Overload.
Самый распространенный тип NAT. Стоит в каждом домашнем роутере.

Идея: много внутренних IP → один внешний IP + уникальные порты.

Таблица трансляций:

Локальный IP	Локальный порт	Публичный IP	Внешний порт
192.168.1.2	1000	85.140.10.5	5000
192.168.1.3	1000	85.140.10.5	5001
192.168.1.4	1000	85.140.10.5	5002

Как работает:
1. Устройство 192.168.1.2:1000 отправляет пакет на сервер.
2. Роутер меняет IP на 85.140.10.5 и порт на 5000.
3. Запоминает соответствие в таблице.
4. Ответ на порт 5000 → роутер отдает устройству 192.168.1.2:1000.

Система NAT: преимущества, недостатки и Port Forwarding

Преимущества NAT:

- Экономия публичных IPv4-адресов
- Скрытие внутренней структуры сети (безопасность)
- Гибкость: можно менять внутреннюю адресацию без уведомления провайдера

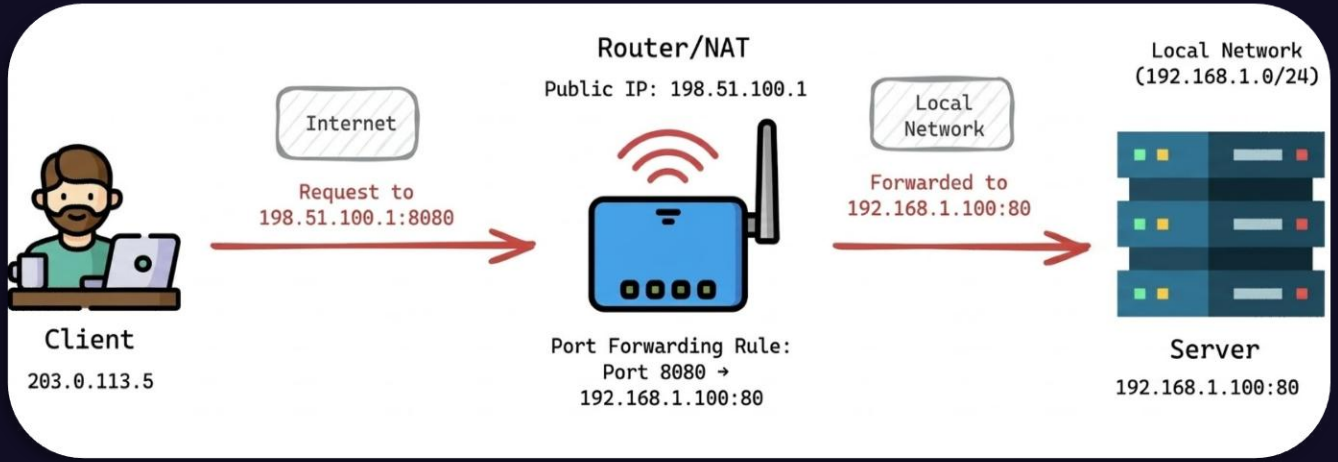
Недостатки NAT:

- Нарушение сквозной связи (End-to-End)
- Сложности с VoIP, P2P-сетями, онлайн-играми
- Внешние устройства не могут сами инициировать соединение
- Усложняется туннелирование (VPN, IPSec)

Port Forwarding

Решение проблемы: Port Forwarding (проброс портов)

- Настройка на роутере: внешний порт → внутренний IP:порт
- Пример: все запросы на внешний порт 8080 → перенаправлять на 192.168.1.10:80



Система NAT: итоговая схема работы

Полный цикл работы NAT (PAT):

1. Устройство (192.168.1.2) отправляет запрос на сервер (8.8.8.8:443).
2. Пакет приходит на роутер (шлюз).
3. Роутер меняет:
   - Source IP: 192.168.1.2 → 85.140.10.5 (публичный)
   - Source Port: 54321 → 5000 (свободный внешний)
4. Запись в таблице: 192.168.1.2:54321 ↔ 85.140.10.5:5000
5. Пакет уходит в интернет.
6. Сервер отвечает на 85.140.10.5:5000.
7. Роутер смотрит в таблицу, находит соответствие.
8. Меняет обратно: 85.140.10.5:5000 → 192.168.1.2:54321.
9. Пакет доходит до устройства.

Спасибо за внимание