Сети

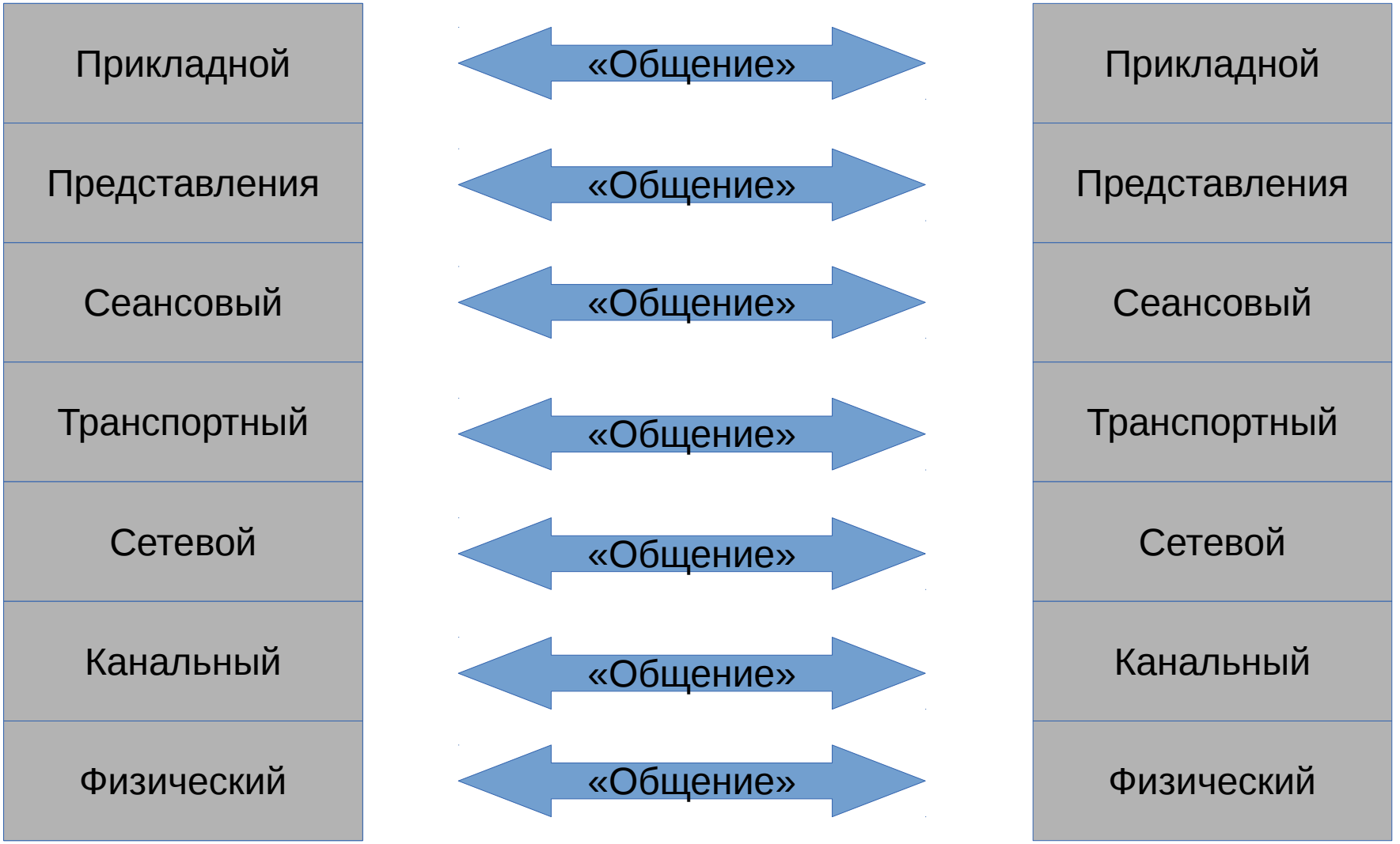
Пирамида для сетей

1) Аппаратная реализация передачи данных: NRZ/NRZI и т.д.
2) Протоколы, алгоритмы: предмет рассмотрения текущей лекции
3) Абстракции ОС/API: предмет рассмотрения следующей лекции

ISO/OSI


Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический
Передача
Прием

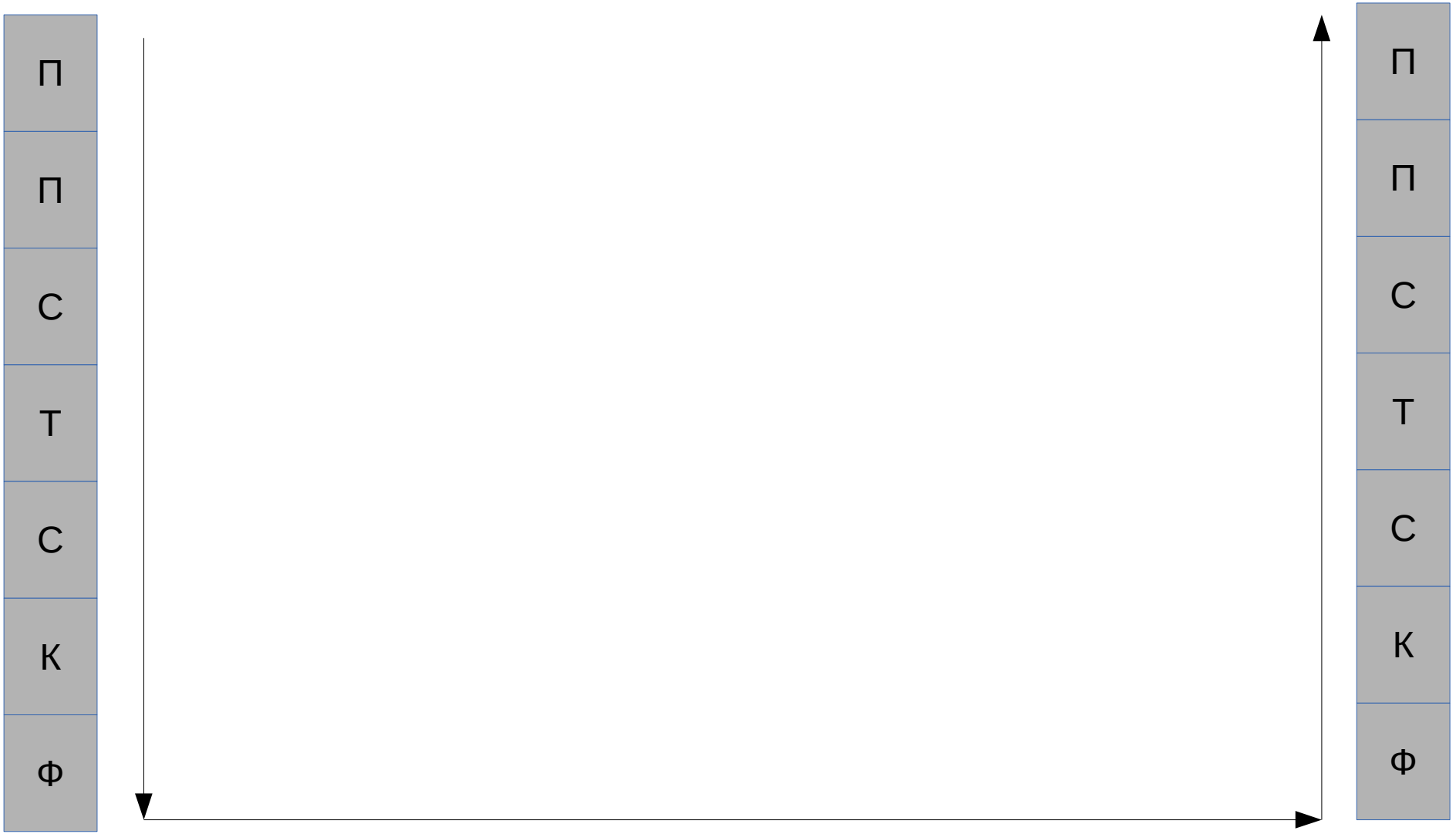
Горизонтальное взаимодействие



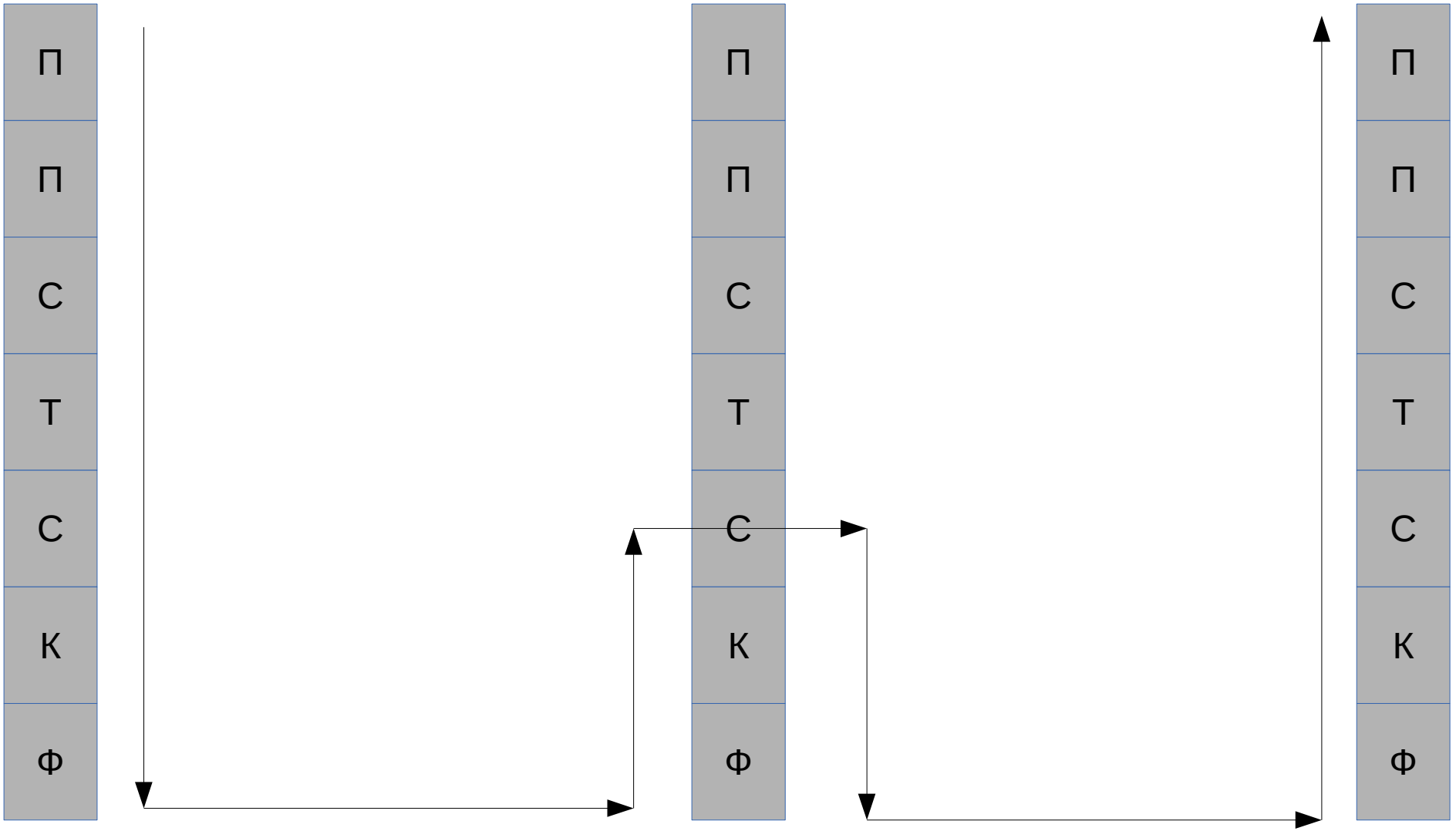
Назначение, примеры

- Физический: передача, кодирование сигнала (биты). 802.11 (WiFi)
- Канальный: передача фреймов. Целостность. Ethernet, PPP
- Сетевой: организация (наикратчайшего) пути передачи данных. IP(+IPv6), IPX (Novell)
- Транспортный: организация надежной передачи данных. TCP/UDP, SPX (Novell)
- Сеансовый: установление/возобновление сеанса. RPC
- Представление: преобразование в единый формат (BE,LE)
- Прикладной (Приложений): обеспечение взаимодействия программ. HTTP, SMTP

В одной сети



В разных сетях



Сетевое оборудование и уровни

- L1: концентратор (hub): транслирует все фреймы, которые приходят с одного порта на все другие
- L2: коммутатор (switch), мост (bridge): просматривает пакеты, запоминает MAC-адреса, отправляет нужному
- L3: маршрутизатор: просматривает пакеты, собирает в IP, принимает решение и на уровне IP-адреса

Протоколы и уровни

- Протокол работает на уровне K:
  - Для работы требуется K-1 уровень
- Протокол реализует уровень K:
  - Работает на уровне K
  - Используется для уровня K+1

Примеры

- ARP (Address Resolution Protocol):
  - служебный, использует ethernet
- AoE (ATA over Ethernet):
  - использует ethernet
- IP:
  - использует ethernet
  - реализует Сетевой уровень

Текущая реальность

- Стек TCP/IP:
  - Сетевого доступа (Канальный (Ethernet) + физический)
  - Межсетевого доступа (Сетевой) IP, IGMP (224.x.x.x)
  - Транспортный (TCP/UDP/SCTP)
  - Приложений (все остальное)
- Все остальные — над/между уровнями:
  - VLAN (802.11q): между физическим и канальным
  - PPPoE: между канальным и сетевым
  - IPSec: между сетевым и транспортным
  - SSL: на уровне представления (над транспортным)
  - HTTP/FTP/SMTP: на уровне приложения

Пример

- Письмо:
  - Content-Type: multipart/alternative;
  - ----==_mimepart_532941cfcd90f_7e143fc3e72e09b034488
    - Content-Type: text/plain;
    - Content-Transfer-Encoding: base64
  - ----==_mimepart_532941cfcd90f_7e143fc3e72e09b034488
    - Content-Type: text/html;
- SMTP: telnet smtp.yandex.ru 25
  - ehlo test
  - mail from: <>
  - rcpt to: [адрес получателя]
  - data
  - .

Сетевые диски (NAS)

- На уровне диска/раздела:
  - AoE (ethernet)
  - ISCSI (TCP)
  - FC (FCP) — на своем стеке протоколов
- На уровне директорий:
  - NFS (RPC → UDP/TCP)
  - SMB
- На уровне приложения:
  - FTP/SSH/HTTP

Сетевое взаимодействие на примере TCP/IP

- Устройства: A ↔ B ↔ C
- Сети: N1 (AB), N2 (BC)
- Сетевые карты: N1A, N1B, N2B, N2C
- MAC (N1A) — MAC-адрес сетевой карты N1A
- IP(N1A) — IP-адрес сетевой карты N1A
  - вообще говоря на одной карте может быть несколько адресов
- Пакеты:
  - MAC(кому):IP(кому) # MAC(от кого):IP(от кого)
  - MAC:IP:Port (для TCP/UDP/SCTP/...)

Локальная передача данных

- (… → IP → MAC → кабель)
- ARP-таблица: IP → MAC
  - Если адреса нет, то послать ARP-запрос в сеть:
    - MAC(все):IP(кого ищем) # MAC(свой):IP(свой)
- В ответе:
  - MAC(A):IP(A)#MAC(B):IP(B):: мой MAC=MAC(B)
- A → B:
  - MAC(N1B):IP(N1B) # MAC(N1A):IP(N1A)

Адреса

- IP 10.1.1.10, netmask: 255.255.255.0 (/24):
  - Все: 0.0.0.0
  - Все из этой сети: 10.1.1.255
- MAC:
  - Все: ff:ff:ff:ff:ff:ff

Межсетевая передача

- IP + netmask:
  - Локальная передача или межсетевая?
- Таблица маршрутизации:
  - netstat -rn
  - route add …

Destination Gateway Genmask Flags MSS Window irtt Iface

0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 wlan1

192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan1

- Найти маршрут, послать пакет маршрутизатору

Межсетевая передача: пакеты

- Пусть в таблице маршрутизации A в направлении N2C стоит IP(N1B)
- A: (узнает MAC(N1B), если не знала)
  - MAC(N1B):IP(N2C) # MAC(N1A):IP(N1A)
- B: (имеет право отвергнуть на IP-уровне, т. к. адрес не его, должен знать, что маршрутизатор):
  - MAC(N2C):IP(N2C) # MAC (N2B):IP(N1A)
- C: получает пакет, знает N1A. Обратный маршрут не обязан идти через B

Межсетевая передача: NAT

- Пусть в таблице преобразования маршрутизатора B стоит правило:
  - N2B: IP(N1A) → Ext
- Пусть соединение идет по 80 порту (TCP)
- A: (обратный порт выдает ОС, пусть будет 4000):
  - MAC(N1B):IP(N2C):80 # MAC(N1A):IP(N1A):4000
- B: (видит, что пакет уходит в N2B):
  - Запоминает: IP(N1A):4000 ↔ Ext:5123
  - Посылает: MAC(N2C):IP(N2C) # MAC (N2B):Ext:5123
- C: получает пакет, знает Ext и порт 5123. Обратный маршрут должен пройти через B

NAT: ответ

- C: Посылает ответ (Аналогично найдя, что для Ext маршрутизатором является N2B):
  - MAC(N2B):Ext:5123 # MAC(N2C):IP(N2C):80
- B: (видит, что пакет пришел через N2B):
  - Смотрит: IP(N1A):4000 ↔ Ext:5123
  - Посылает: MAC(N1A):IP(N1A):4000 # MAC (N1B):IP(N2C):80
- A: Получает свой ответ

Сетевое взаимодействие: DHCP

- Поверх UDP
- Клиент (A):
  - MAC(все):IP(все):67 # MAC(A):IP(все):68
- Сервер (ответ):
  - MAC(A):IP(A):68 # MAC (сервера):IP(сервера):67:
    - Твой адрес: IP(A)
    - Сетевая маска: Net(A)
    - Шлюз: IP(Gateway) (не обязательно сервер)
    - Грузиться: IP(Boot-server) (если сетевая загрузка)
    - Файл для загрузки: /A/pxeboot (если сетевая загрузка)
- Если загрузка по сети, то дальнейшее общение A и IP(Boot-server) по TFTP

ARP-атаки

- H атакует A, чтобы выдать себя за B:
  - ARP ответ: MAC(A):IP(A)#MAC(H):IP(B)
- Если A не запрашивал, то:
  - ARP ответ: MAC(A):IP(D)#MAC(H):IP(B)