

# Сеть и сетевые протоколы: L2-сеть



Андрей  
Вахутинский



# Андрей Вахутинский

Заместитель начальника IT-отдела  
АО “ИНТЕКО”

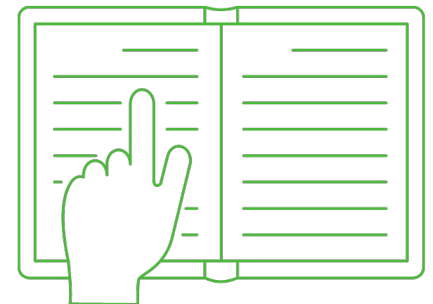


[Андрей Вахутинский](#)

# Предисловие

Эта лекция содержит **основные понятия**, связанные со 2-м уровнем модели OSI (Data link layer / Канальный уровень).

Также вы познакомитесь с основными командами, которые позволяют получать информацию / вносить изменения в настройки ОС на 2-м уровне модели OSI.



---

# План занятия

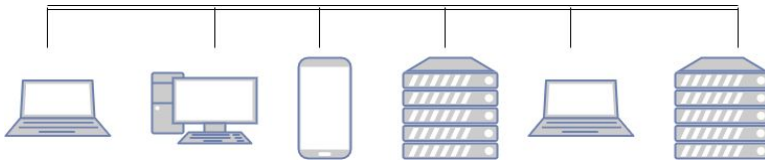
1. [Предисловие](#)
2. [Виды сред передачи данных](#)
3. [Канальный уровень \(OSI\)](#)
4. [VLAN](#)
5. [Spanning Tree Protocol \(STP\)](#)
6. [Address Resolution Protocol \(ARP\)](#)
7. [Итоги](#)
8. [Домашнее задание](#)



# Виды сред передачи данных

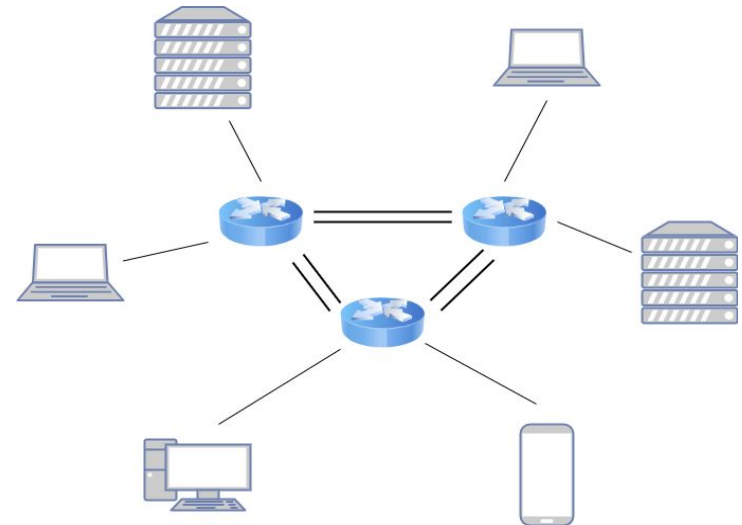
# Виды сред

## Общая медиа (разделяемая среда)



- коллизии
- + не нужны доп.устройства

## Switched (коммутируемая среда)



- цена выше
- + нет коллизий – выше скорость, больше участников <sup>6</sup>

# Домен коллизий

**Домен коллизий** — часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.

Чем больше узлов в таком сегменте — тем выше вероятность коллизий.

Для разделения домена коллизий применяются коммутаторы.

---

# Сетевые устройства и домен коллизий

Сетевые устройства, работающие на канальном уровне модели OSI, могут продлевать, либо ограничивать домен коллизий.

**Устройства первого уровня OSI** (концентраторы, повторители) только ретранслируют любой сигнал, поступающий из среды передачи, и **продлевают** домен коллизий.

**Устройства второго уровня OSI** (мосты, коммутаторы), **разделяют** домен коллизий.





# Канальный уровень (OSI)

---

# Канальный уровень

Протоколы канального уровня отвечают за доставку данных **внутри** одного сегмента сети.

**Стандарт для сетей Ethernet** имеет название IEEE 802.3 и детальное описание приведено в [документе](#).

**Сегмент сети**, согласно IEEE 802.3, – это электрически соединенные устройства, использующие общую среду. Сегменты соединяются в сеть при помощи повторителей или коммутаторов

---

## Канальный уровень

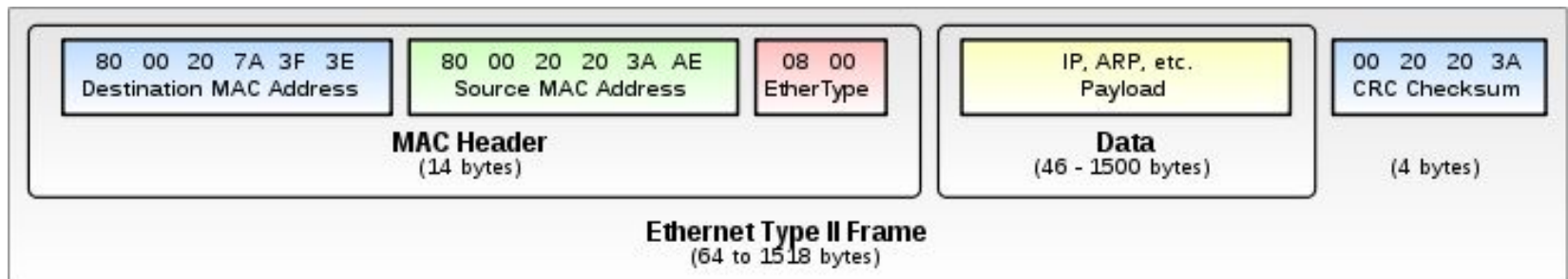
Все узлы внутри одного сегмента имеют доступ друг к другу при помощи аппаратных адресов и образуют широковещательный домен.

Для IEEE 802.3 такой адрес называется **MAC-адресом**. MAC-адрес «зашивается» в сетевые карты (но может быть изменён).

**Широковещательный домен** – метод доставки сообщений, при котором сообщение получают сразу все участники обмена (связи).  
Нужное сообщение фильтруется самим узлом по MAC-адресу.

# Формат кадра Ethernet

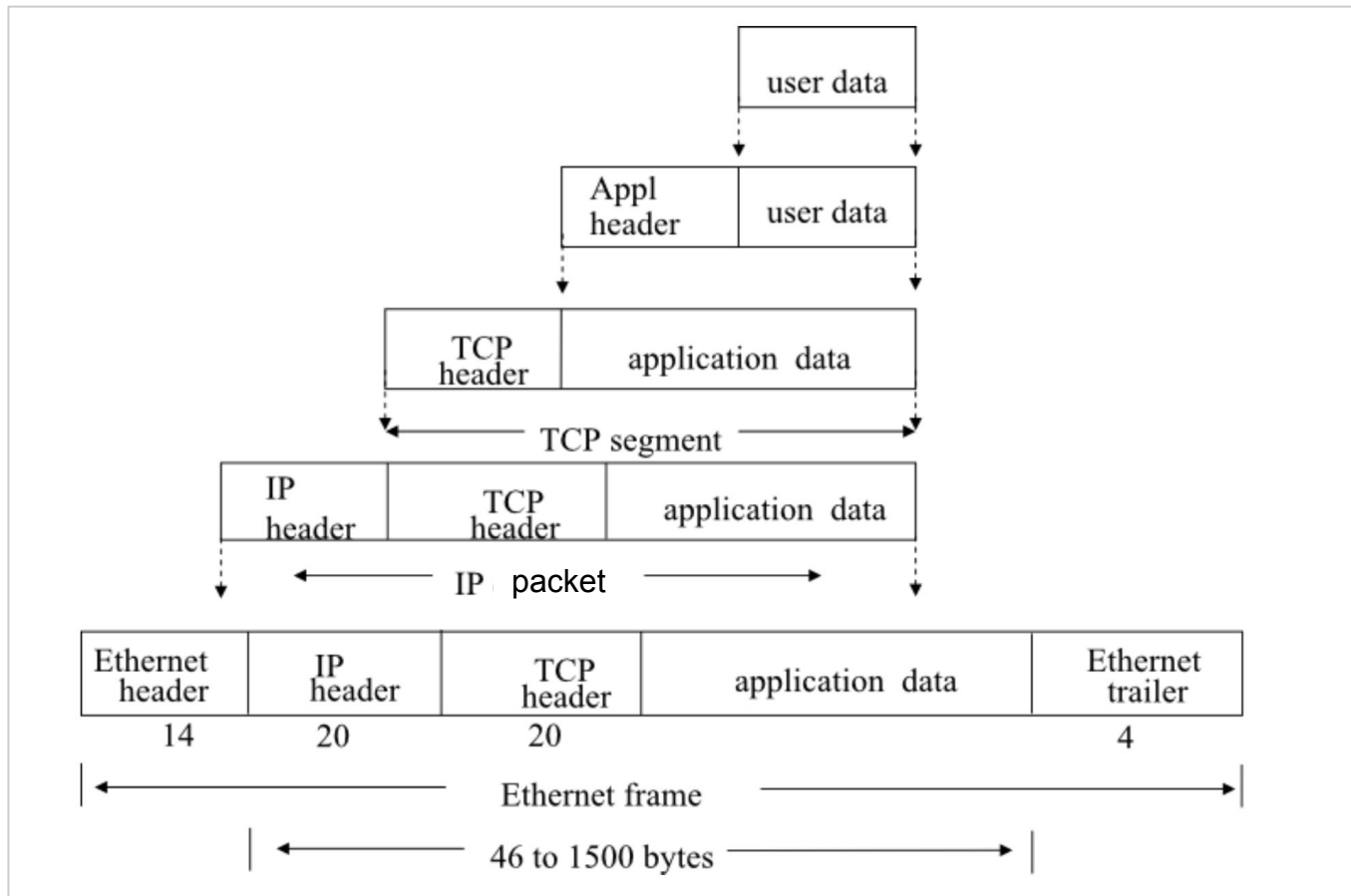
Формат кадра Ethernet имеет вид:



- **MACs** – адрес приемника и отправителя;
- **Ether Type** – тип Ethernet либо размер Payload;
- **Payload** – данные;
- **CRC** – контрольная сумма.

# MTU




TCP/IP Illustrated, Vol. 1



\*MTU (Maximum Transmission Unit) – размер полезных данных в одном фрейме (размер фрейма минус заголовки Ethernet, минус трейлер Ethernet),

---

# Типы передачи трафика

- **Broadcast трафик** – процесс отправки пакета от одного хоста *ко всем хостам в сети*;  
 Пример: служебный трафик.
- **Unicast трафик** – процесс отправки пакета от одного хоста *к другому хосту*;  
 Пример: общение 2-х компьютеров.
- **Multicast трафик** – процесс отправки пакета от одного хоста *к некоторой ограниченной группе хостов*.  
 Пример: видео по подписке (IPTV).

---

## Аналогии типов передачи трафика

Представим, что у нас есть жилой дом на несколько подъездов и у этого дома есть доска объявлений, на которой управляющая компания информирует жильцов своего дома.

Если в объявление будет написано «всем жильцам дома», то это будет похоже на **broadcast**.

Если написано «жильцам третьего этажа» или «жильцам второго подъезда», то это будет похоже на **multicast**.

Письмо в почтовый ящик – похоже на **unicast**.



**VLAN**



---

# Локальная сеть

**Локальная сеть** (LAN) – компьютерная сеть, расположенная в небольшой области, например, в офисе, университете, здании.

Локальная сеть, как правило, разбивается коммутаторами на несколько сегментов (VLAN), что *облегчает администрирование и уменьшает широковещательный трафик внутри сети.*

**Виртуальная LAN** (VLAN) – логически обособленный сегмент локальной сети внутри одной физической сети.

---

## Виртуальная LAN (VLAN)

**VLAN** – технология, которая позволяет строить виртуальные сети с независимой от физических устройств топологией.

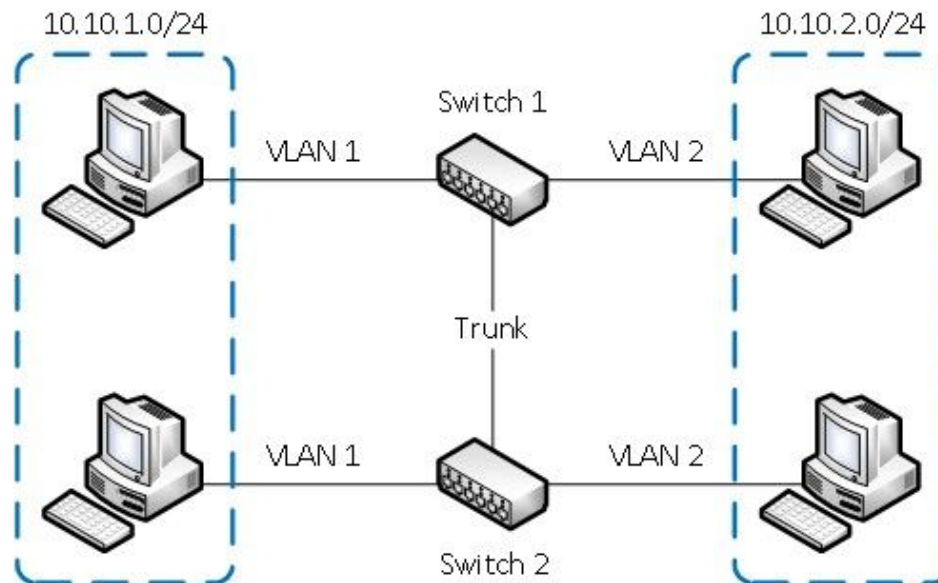
Например, можно объединить в одну сеть отдел компании, сотрудники которого работают в разных зданиях и подключены к разным коммутаторам. или наоборот, создать отдельные сети для устройств, подключённых к одному коммутатору, если этого требует политика безопасности.



# Возможности VLAN

→ Объединить в единую сеть группы компьютеров, подключённых к разным коммутаторам.

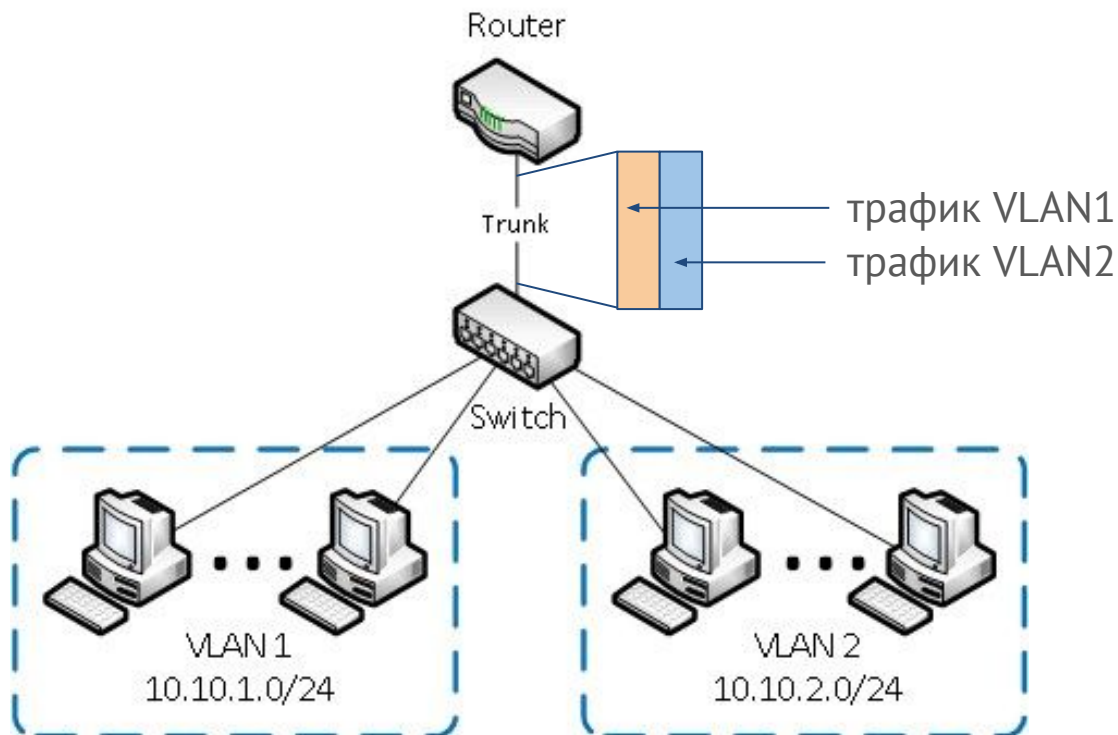
Компьютеры в **VLAN 1** будут взаимодействовать между собой, хотя подключены к разным физическим коммутаторам, при этом сети **VLAN 1** и **VLAN 2** будут невидимы друг для друга.



# Возможности VLAN

→ Разделить на разные сети компьютеры, подключённые к одному коммутатору.

При этом устройства в **VLAN 1** и **VLAN 2** не смогут напрямую взаимодействовать между собой.



---

# Преимущества VLAN

- сокращение числа широковещательных запросов, которые снижают пропускную способность сети;
- повышение безопасности каждой виртуальной сети.

Работники одного отдела офиса не смогут отслеживать трафик отделов, не входящих в их VLAN, и не получат доступ к их ресурсам.

- создание новой виртуальной сети без прокладки кабеля и покупки коммутатора;
- объединение в одну сеть компьютеров, подключенных к разным коммутаторам;
- упрощение сетевого администрирования.

# Пример VLAN

```
lsmod | grep 8021q  
sudo modprobe 8021q # если появляется ошибка "Maybe you need to load the 8021q module"
```

```
# ip link add link eth0 name eth0.10 type vlan id 10  
# ip -d link show eth0.10
```

```
[root@localhost ~]# ip -d link show eth0.10  
4: eth0.10@eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000  
    link/ether 52:02:a4:e3:26:b5 brd ff:ff:ff:ff:ff:ff promiscuity 0  
    vlan protocol 802.1Q id 10 <REORDER_HDR> addrngenmode eui64 numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535  
[root@localhost ~]#
```

```
# ip addr add 192.168.1.200/24 brd 192.168.1.255 dev eth0.10  
# ip link set dev eth0.10 up  
  
# ip link set dev eth0.10 down  
# ip link delete eth0.10
```

# Пример VLAN

```
lsmod | grep 8021q  
sudo modprobe 8021q # если появляется ошибка "Maybe you need to load the 8021q module"
```

```
# nano /etc/netplan/01-netcfg.yaml  
network:  
  version: 2  
  ethernet:  
    eth0:  
      dhcp4: true  
  vlans:  
    vlan200:  
      id: 200  
      link: eth0  
      dhcp4: no  
      addresses: [192.168.200.2/24]  
      gateway4: 192.168.200.1  
      routes:  
        - to: 192.168.100.1/24  
          via: 192.168.200.3  
          on-link: true
```

```
# netplan apply
```



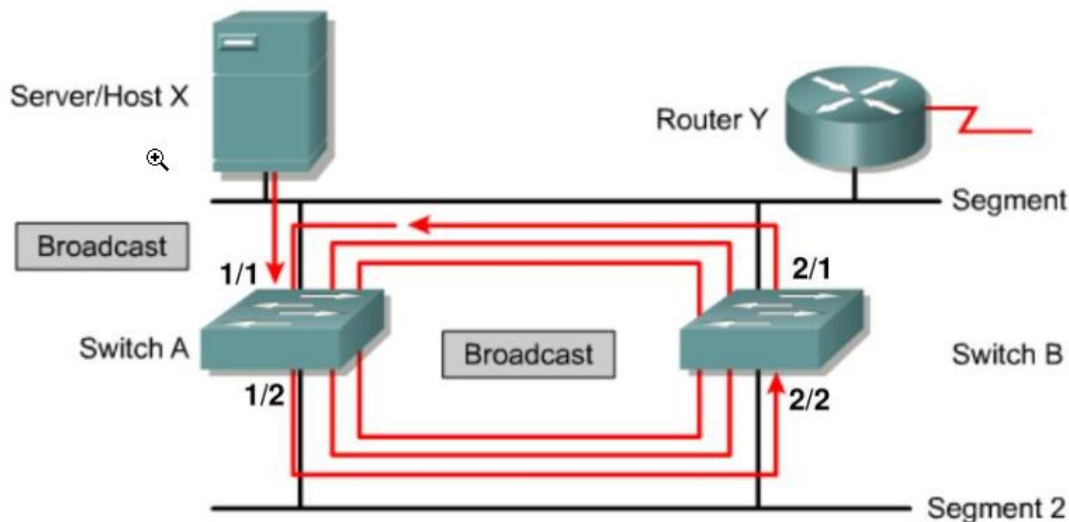
# Spanning Tree Protocol (STP)



# Broadcast шторм

Размножение широковещательных сообщений активным сетевым оборудованием приводит к экспоненциальному росту их числа и парализует работу сети.

Считается нормальным, если широковещательные пакеты составляют не более 10 % от общего числа пакетов в сети.

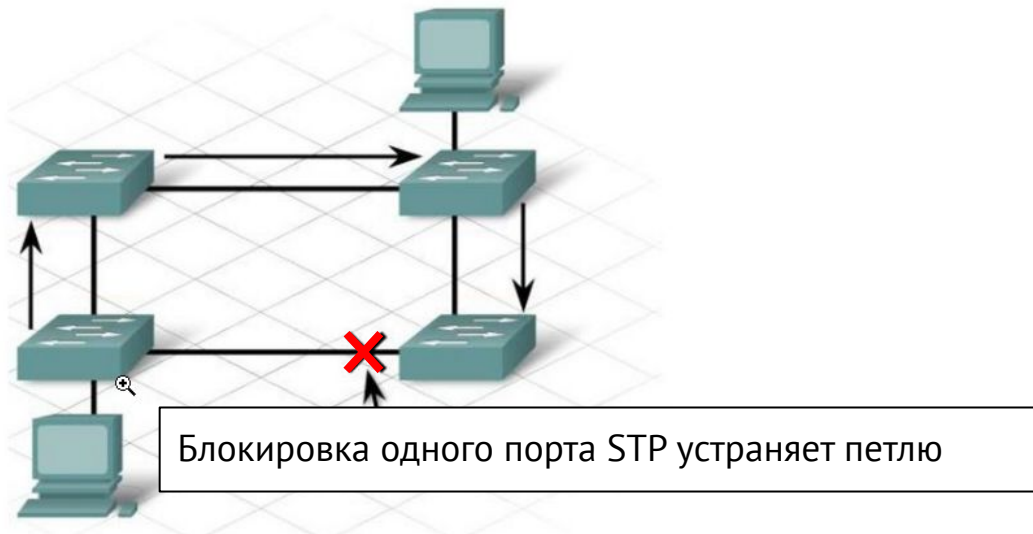


# STP

Чтобы не происходило заикливания, петлю нужно разорвать.

Для этого придумали специальный протокол – **Spanning Tree Protocol** (STP).

Его задача – выбрать порты, которые нужно отключить.



---

# Необходимость двухуровневой адресации

## Разделяемая среда – одноуровневая адресация.

- вся сеть – локальная, поэтому только адреса локальной сети;
- «все слышат всех», проблем с доставкой до адресата нет.

## Выделенная среда – одноуровневая адресация.

- появляется дополнительное устройство – коммутатор, который обеспечивает выделенный канал между своим портом и устройством и понимает кому предназначаются данные (отсутствие коллизий);
- все уже не слышат всех, коммутатор знает какой адрес находится за каким физическим портом.

# Необходимость двухуровневой адресации

Но что будет, если в коммутатор уже невозможно подключить новых участников сети, или они удалены по расстоянию?

➔ Можно сделать несколько локальных сетей и объединить их.

**Двухуровневая адресация** – необходимость при объединении нескольких сетей.



---

## MAC и IP



Но как между собой связаны MAC и IP-адреса?

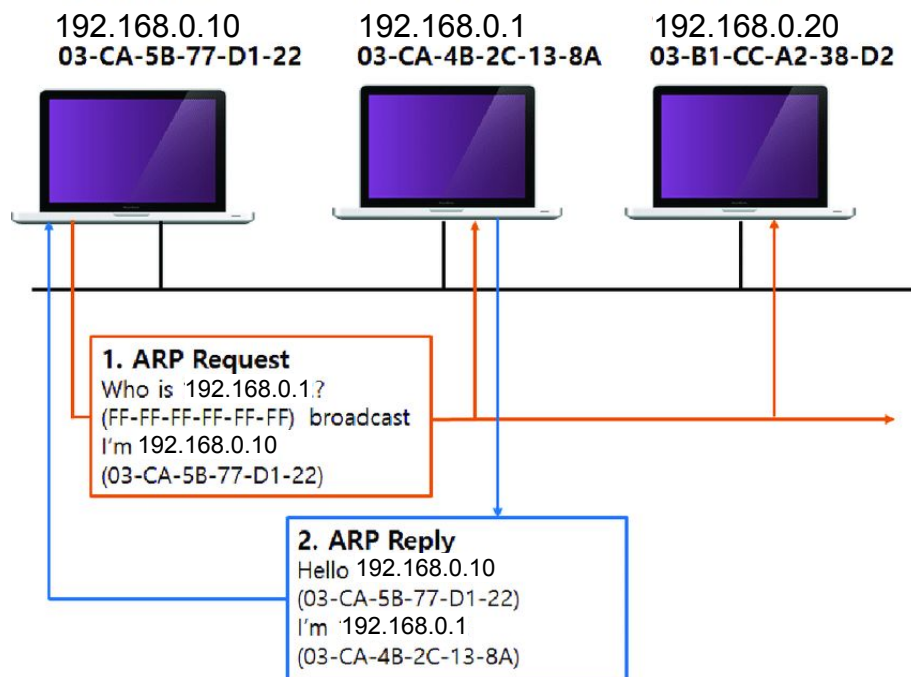
Как можно из одного получить другой – и наоборот?



# Address Resolution Protocol (ARP)

# Address Resolution Protocol (ARP)

**ARP** (протокол определения адреса) – в стеке протоколов TCP/IP определяет IP-адрес по MAC-адресу узла и наоборот.



# ARP таблица в Linux

## Просмотр ARP таблицы

```
# ip neigh show dev eth1

# ping -c 1 192.168.11.12
PING 192.168.11.12 (192.168.11.12) 56(84) bytes of data.
64 bytes from 192.168.11.12: icmp_seq=1 ttl=64 time=1.58 ms
--- 192.168.11.12 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.588/1.588/1.588/0.000 ms

# ip neigh show dev eth1
192.168.11.12 lladdr 08:00:27:23:22:97 REACHABLE
```

Если узел **192.168.11.10** через интерфейс **eth1** осуществит сетевое взаимодействие с узлом **192.168.11.12** (например, с помощью утилиты **ping**), то в его ARP-таблице появится новая запись, которую можно просмотреть командой **ip neigh show** (параметр **dev** указывает фильтровать записи относящиеся к интерфейсу **eth1**).



---

# ARP таблица в Linux

## Добавление статической записи

```
# ip neigh add 192.168.11.100 lladdr 00:00:00:00:00:AA dev eth1  
  
# ip neigh show dev eth1  
192.168.11.100 lladdr 00:00:00:00:00:aa PERMANENT
```

Обратите внимание: на статический характер записи указывает ключевое слово PERMANENT, в отличие от REACHABLE, означающий динамическую запись

## Удаление записи

```
# ip neigh del 192.168.11.100 dev eth1
```

# ARP таблица в Linux

Все тоже самое можно делать с помощью «традиционной» утилиты ARP

```
# arp -s 192.168.11.100 00:00:00:00:00:AA
# arp -i eth1
Address HWtype HWaddress Flags Mask Iface
192.168.11.100 ether 00:00:00:00:00:aa CM eth1
# arp -d 192.168.11.100
```

# arping

## Опрос узлов локальной сети на L2

```
$ ping -c 1 10.0.2.3
PING 10.0.2.3 (10.0.2.3) 56(84) bytes of data.
..
--- 10.0.2.3 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

$ sudo arping -c 1 10.0.2.3
60 bytes from 52:54:00:12:35:03 (10.0.2.3): index=0 time=7.346 usec
--- 10.0.2.3 statistics ---
1 packets transmitted, 1 packets received, 0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.007/0.007/0.007/0.000 ms
```

Если протокол ICMP, с помощью которого можно протестировать работоспособность удалённых узлов, зафильтрован, мы можем использовать утилиту APRING, которая работает на 2-м уровне модели OSI.

# tcpdump

## Просмотр трафика L2

```
# sudo tcpdump -i any arp -nn -v -A -e
```

- С опцией `-e` программа tcpdump будет печатать заголовки канального уровня в каждой выведенной строке.

➡ Это может использоваться, например, для показа аппаратных адресов MAC для таких протоколов как Ethernet и IEEE 802.11.

- С опцией `-A` команда tcpdump будет отображать на экране содержимое пакетов в формате ASCII.
- ...

# tcpdump

## Просмотр трафика L2

```
# sudo tcpdump -i any arp -nn -v -A -e
```

- Опция `-v` при парсинге и выводе печатает чуть больше информации.

 Например, добавляет время жизни пакета, идентификацию, общую длину и опции в IP пакетах.

- Опция `-nn` отображает порты и ip-адреса цифрами вместо имён (localhost, ssh, http, и т.д.)




# Итоги

---

# Итоги

## Сегодня мы узнали:

- основы L2;
- о взаимодействии между L2 и L3;
- основные команды ОС на 2-м уровне модели OSI.

 Теперь мы умеем проводить базовую диагностику связности на 2-м уровне модели OSI.



# Домашнее задание



---

# Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

**Задавайте вопросы и  
пишите отзыв о лекции!**

**Андрей Вахутинский**