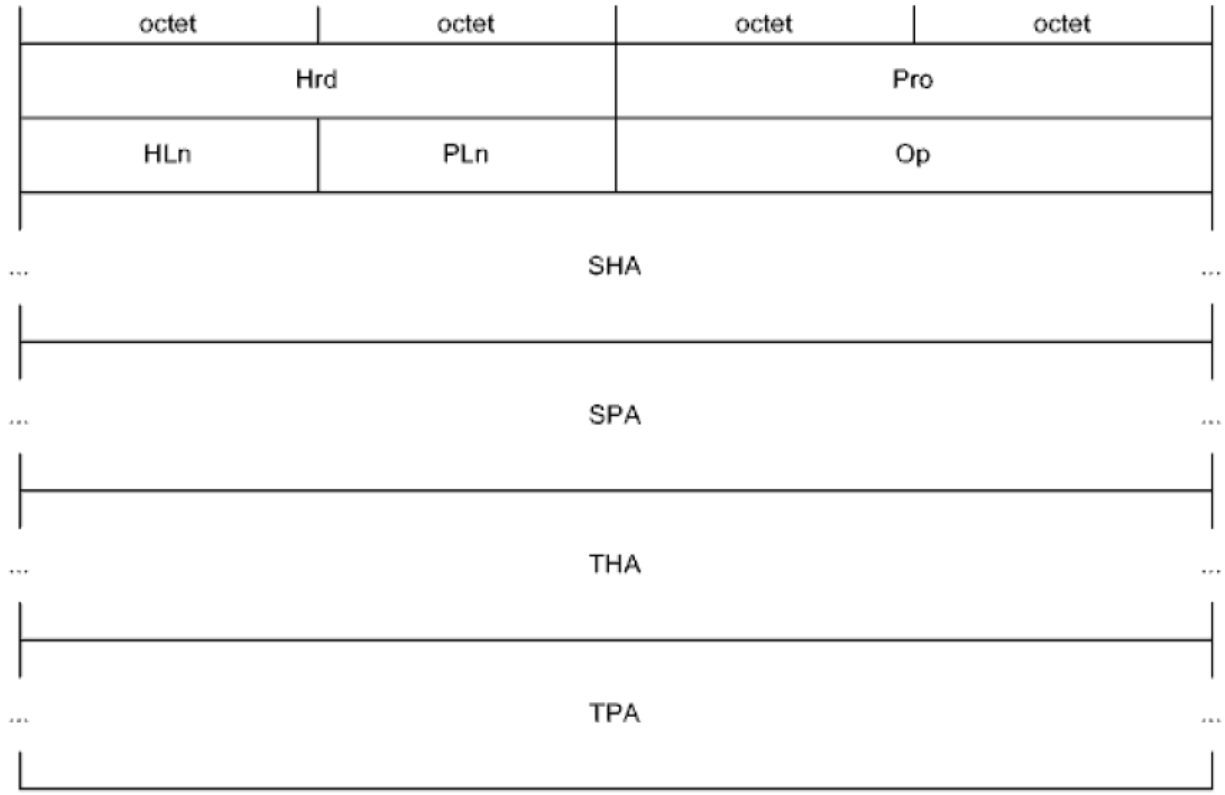
46 Протокол ARP

Группа протоколов под названием ARPs (Address Resolution Protocols) предназначена для восстановления соответствий между MAC-адресами и IP-адресами.

Под прямым преобразованием, собственно ARP (RFC 826), понимают нахождение MAC-адреса по IP-адресу.

Обратное преобразование выполняется по протоколу RARP (Reverse ARP).



Формат пакета ARP

Поля:

Hrd (Hardware) -- тип оборудования (1 -- Ethernet).

Pro (Protocol) -- протокол (800h -- IP).

HLn (Hardware address Length) -- длина аппаратного (физического) адреса (в байтах, 6 -- Ethernet).

PLn (Protocol address Length) -- длина протокольного (логического) адреса (в байтах, 4 -- IP).

5. Op (Opcode) -- код операции: 1 -- Request -- запрос, 2 -- Reply -- ответ (и некоторые другие).

6. SHA (Sender Hardware Address) -- аппаратный адрес станции-отправителя (запрашивающей либо отвечающей на запрос).

7. SPA (Sender Protocol Address) -- протокольный адрес станции-отправителя.

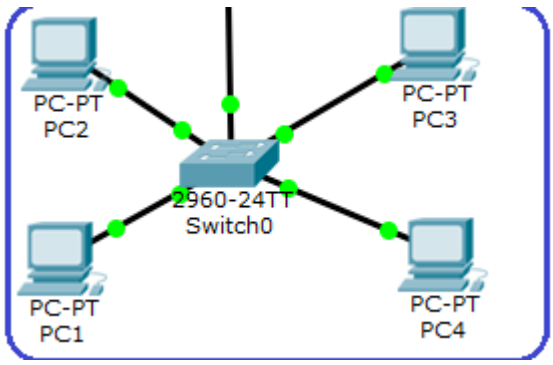
8. THA (Target Hardware Address) -- аппаратный адрес станции-получателя.

9. TPA (Target Protocol Address) -- протокольный адрес станции-получателя.

аппаратный адрес – MAC

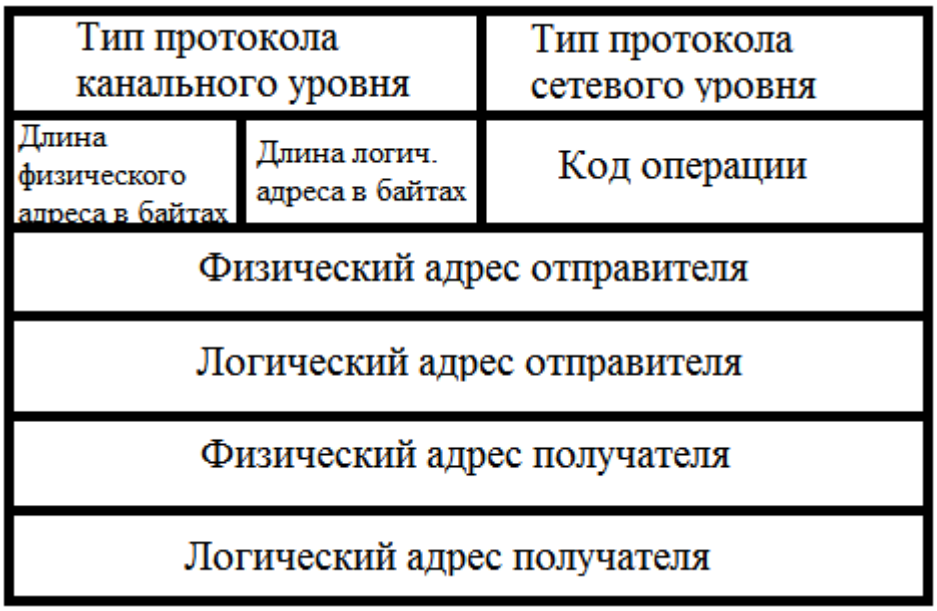
протокольный адрес – IP

Пример использования мб запомнишь и можно будет выебнуться)



Мы хотим пинганути компьютер PC4 и мы знаем что у него IP 192.168.1.4, а мы сидим за компьютером PC1 и у нас IP 192.168.1.1.

Но тут ping сталкивается с проблемой. Он не знает MAC-адрес получателя. То есть, адрес канального уровня. Для этого он использует протокол ARP, который сможет опросить участников сети и узнать MAC-адрес. Мы про него вскользь говорили в предыдущей статье. Давайте поговорим о нем подробнее. Не буду изменять традиции. Картинку в студию!



1) Тип протокола канального уровня (Hardware type). Думаю понятно из названия, что тут указывается тип канального уровня. Мы пока рассматривали только Ethernet. Его обозначение в этом поле — 0x0001.

2) Тип протокола сетевого уровня (Protocol type). Тут, аналогично, указывается тип сетевого уровня. Код IPv4 — 0x0800.

3) Длина физического адреса в байтах (Hardware length). Если это MAC-адрес, то размер будет 6 байт (или 48 бит).

4) Длина логического адреса в байтах (Protocol length). Если это IPv4-адрес, то размер будет 4 байта (или 32 бита).

5) Код операции (Operation). Код операции отправителя. Если это запрос, то код 0001. В случае ответа — 0002.

6) Физический адрес отправителя (Sender hardware address). MAC-адрес отправителя.

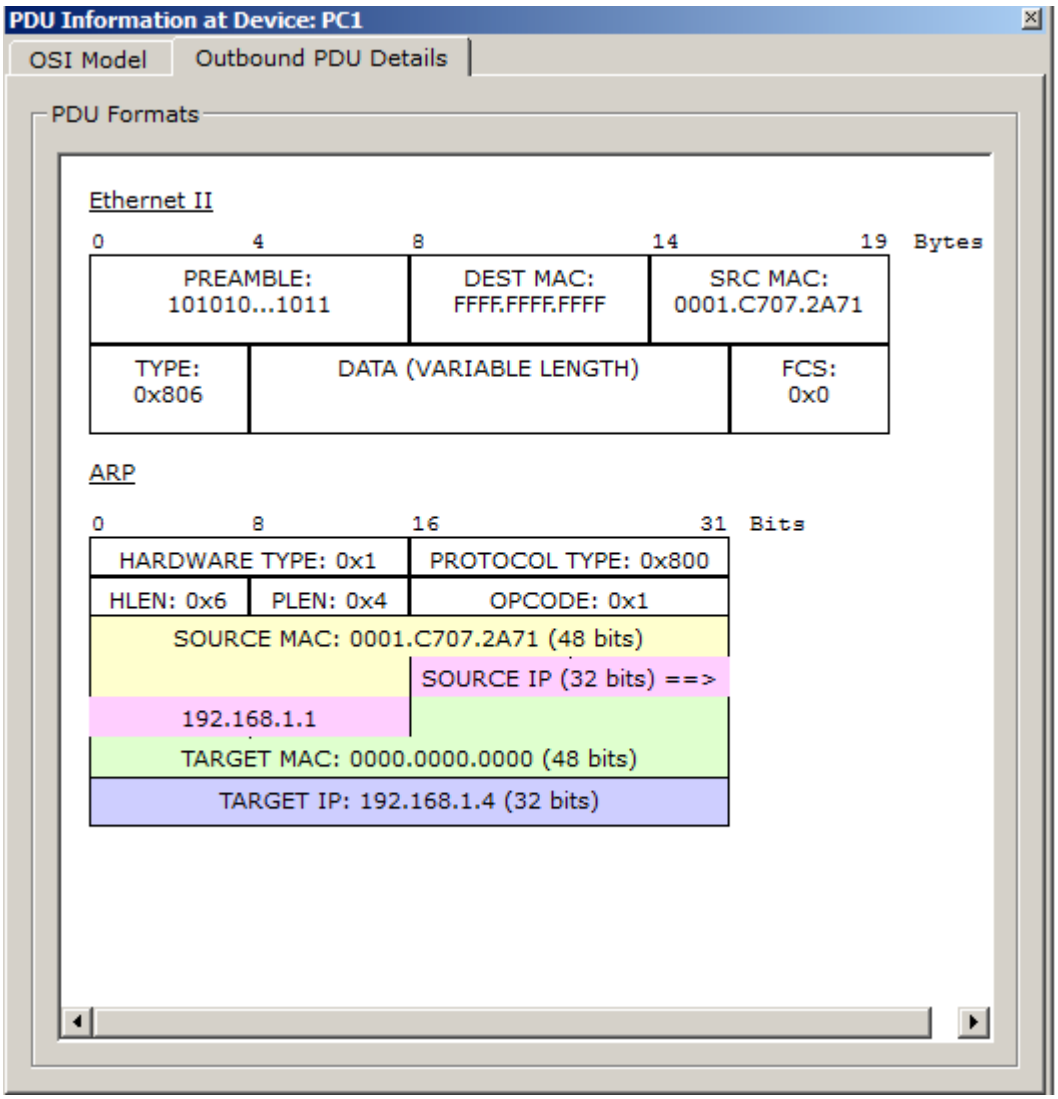
7) Логический адрес отправителя (Sender protocol address). IP-адрес отправителя.

8) Физический адрес получателя (Target hardware address). MAC-адрес

получателя. Если это запрос, то, как правило, адрес неизвестен и это поле остается пустым.

9) Логический адрес получателя (Target protocol address). IP-адрес получателя

Теперь, когда мы знаем, из чего он состоит, можно посмотреть на его работу в CPT. Кликаю по второму конверту и наблюдаю следующую картину.



И вот протокол ARP во всей красе. На 2-ом уровне работает протокол Ethernet. Остановимся и посмотрим на его поля.

1) Преамбула — здесь битовая последовательность, которая говорит о начале кадра.

2) Далее идет MAC-адрес источника и получателя. В адресе источника записан MAC-адрес компьютера, который является инициатором, а в адресе получателя записан широковещательный

адрес FF-FF-FF-FF-FF-FF (то есть для всех узлов в канальной среде).

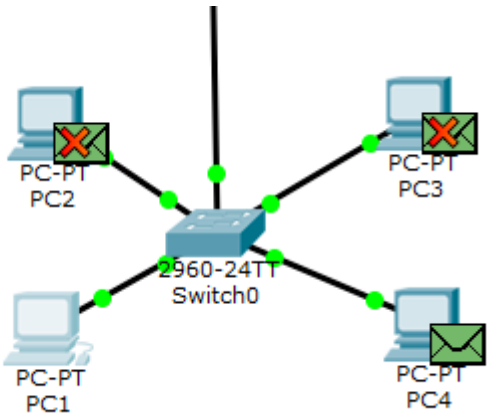
3) Тип — здесь указан вышестоящий протокол. Код 0x806 означает, что выше стоит ARP. Я, если честно, не могу точно сказать, на каком уровне он работает. В разных источниках указано по-разному. Кто то говорит, что на 2-ом уровне OSI, а кто-то говорит, что на 3-ем. Я считаю, что он между ними работает. Так как тут есть адреса, присущие каждому из уровней.

Про данные и чек-сумму много говорить не буду. Данные здесь никак не указаны, а чек-сумма нулевая.

Поднимаемся чуть повыше и здесь протокол **ARP**.

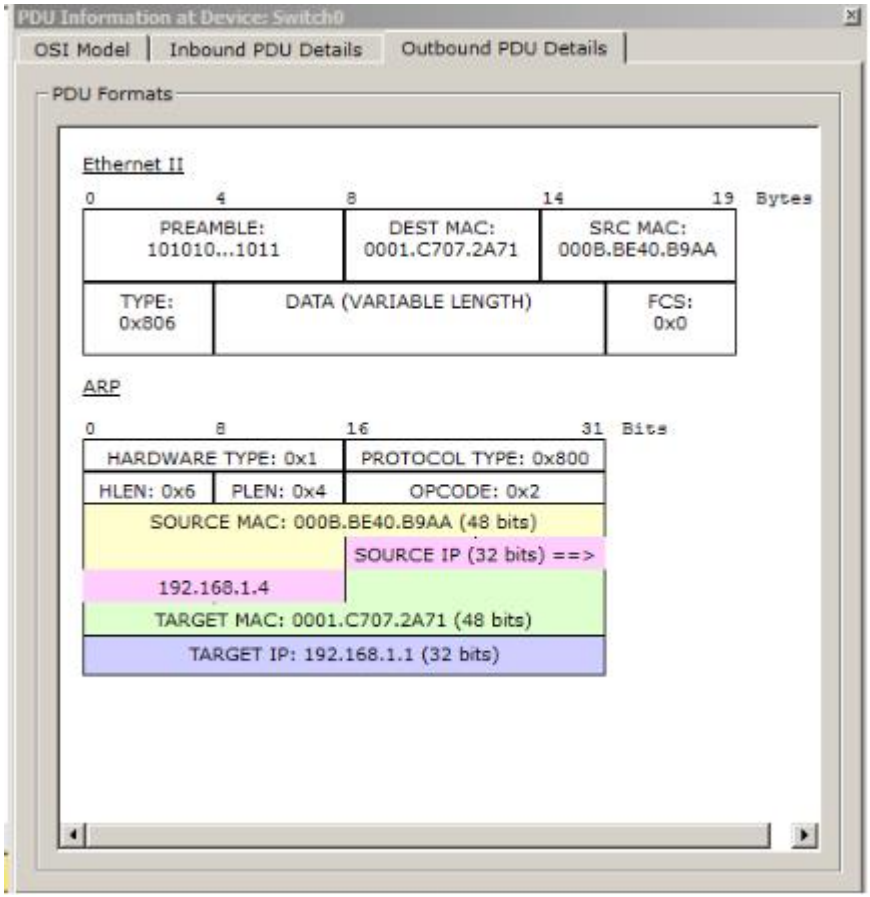
1) Hardware Type — код канального уровня. CPT убрала лишние нули и вставила 0x1 (тоже, что и 0x0001). Это Ethernet.
2) Protocol Type — код сетевого уровня. 0x800 — это IPv4.
3) HLEN — длина физического адреса. 0x6 означает 6 байт. Все верно (MAC-адрес занимает 6 байт).
4) PLEN — длина сетевого адреса. 0x4 означает 4 байта (IP-адрес занимает 4 байта).
5) OPCODE — код операции. 0x1 означает, что это запрос.
6) Source Mac — здесь MAC-адрес отправителя. Можно сравнить его с адресом в поле протокола Ethernet и убедиться в правильности.
7) Source IP — IP-адрес отправителя.
8) Target MAC — так как это запрос и канальный адрес не известен, то он пустой. CPT показала его нулями, что равносильно.
9) Target IP — IP-адрес получателя. Как раз тот адрес, который пингуем.

Посмотрим, что будет происходить дальше в сети.



Протокол ARP опрашивает все хосты в локальной сети и только один отвечает на этот запрос. Это PC4. Посмотрим, чем он ответит.

1) В поле источника протокола Ethernet теперь записан MAC-адрес PC4, а в поле назначения MAC-адрес инициатора, то есть PC1.
2) В поле OPCODE теперь значение 0x2, то есть ответ.
3) Поменялись поля логических и физических адресов в протоколе ARP. Source MAC и Destination MAC аналогичны тем, что в протоколе Ethernet. В поле Source IP — адрес 192.168.1.4 (PC4), а в поле Destination IP — адрес 192.168.1.1 (PC1).



Как только эта информация достигнет PC1, он сразу формирует ICMP-сообщение, то есть ping.

Источник лекция 8

https://habr.com/ru/post/308636/