МДК.02.02 Организация администрирования компьютерных сетей

3-курс

Занятие 06

Порядок назначения IP-адресов

Порядок назначения IP-адресов

По определению схема IP-адресации должна обеспечивать уникальность нумерации сетей, а также уникальность нумерации узлов в пределах каждой из сетей.

Следовательно, процедуры назначения номеров как сетям, так и узлам сетей должны быть централизованными.

Рекомендуемый порядок назначения IP-адресов дается в спецификации RFC 2050.

Назначение адресов автономной сети

Назначение адресов автономной сети

Когда дело касается сети, являющейся частью Интернета, уникальность нумерации может быть обеспечена только усилиями специально созданных для этого центральных органов.

В небольшой же автономной IP-сети условие уникальности номеров сетей и узлов может быть выполнено «вручную» сетевым администратором.

В этом случае в распоряжении администратора имеется всё адресное пространство, так как совпадение IP-адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий.

Назначение адресов автономной сети

Администратор может выбирать адреса произвольным образом, соблюдая лишь синтаксические правила и учитывая ограничения на особые адреса.

Однако при таком подходе исключена возможность в будущем подсоединить данную сеть к Интернету.

Действительно, произвольно выбранные адреса данной сети могут совпасть с централизовано назначенными адресами Интернета.

Для того чтобы избежать коллизий, связанных с такого рода совпадениями, в стандартах Интернета определено несколько диапазонов так называемых **частных адресов**, рекомендуемых для автономного использования.

Назначение адресов автономной сети

Среди них:

□ в классе A — сеть 10.0.0.0;

□ в классе B — диапазон из 16 номеров сетей (172.16.0.0-172.31.0.0);

□ в классе C — диапазон из 255 сетей (192.168.0.0-192.168.255.0).

Эти адреса, исключенные из множества централизованно распределяемых, составляют огромное адресное пространство, достаточное для нумерации узлов автономных сетей практически любых размеров.

Назначение адресов автономной сети

Заметим также, что частные адреса, как и при произвольном выборе адресов, в разных автономных сетях могут совпадать.

В то же время использование частных адресов для адресации автономных сетей делает возможным их корректное подключение к Интернету.

Применяемые при этом специальные технологии подключения исключают коллизии адресов.

Например, такой технологией является NAT.

NAT (Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов

Централизованное распределение адресов

Централизованное распределение адресов

В больших сетях, подобных Интернету, уникальность сетевых адресов гарантируется централизованной иерархически организованной системой их распределения.

Номер сети может быть назначен только по рекомендации специального подразделения Интернета.

Главным органом регистрации глобальных адресов в Интернете с 1998 года является неправительственная некоммерческая организация **ICANN** (Internet Corporation for Assigned Names and Numbers).

Централизованное распределение адресов

Эта организация координирует работу региональных отделов, деятельность которых охватывает большие географические площади:

- ARIN (Америка),
- RIPE (Европа),
- APNIC (Азия и Тихоокеанский регион).

Региональные отделы выделяют блоки адресов сетей крупным поставщикам услуг, а те, в свою очередь, распределяют их между своими клиентами, среди которых могут быть и более мелкие поставщики.

Централизованное распределение адресов

Проблемой централизованного распределения адресов является их дефицит.

Уже сравнительно давно очень трудно получить адрес класса B и практически невозможно стать обладателем адреса класса A.

При этом надо отметить, что дефицит обусловлен не только ростом сетей, но и тем, что имеющееся адресное пространство используется нерационально.

Очень часто владельцы сетей класса C расходуют лишь небольшую часть из имеющихся у них 254 адресов.

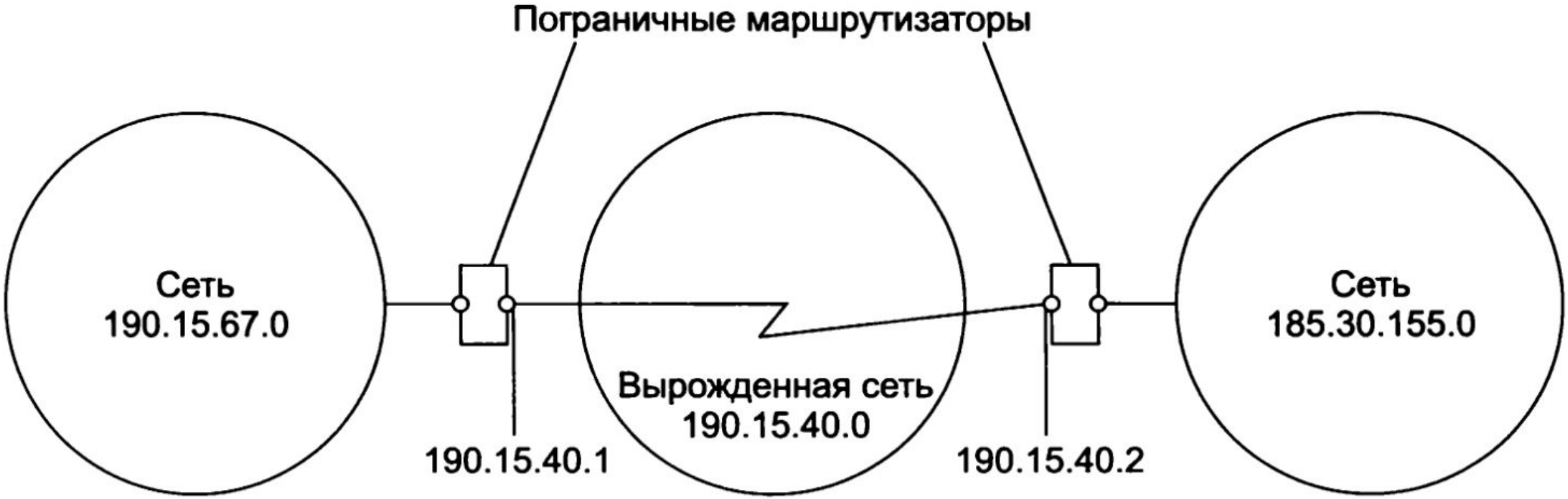
Централизованное распределение адресов

Рассмотрим пример, когда две сети необходимо соединить глобальной связью.

В таких случаях в качестве линии связи используют два маршрутизатора, соединенных по двухточечной схеме (смотри рисунок на следующем слайде).

Для вырожденной сети, образованной линией связи, связывающей порты двух смежных маршрутизаторов, приходится выделять отдельный номер сети, хотя в этой сети всего два узла.

Централизованное распределение адресов



Централизованное распределение адресов

Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы.

Принципиальным решением является переход на новую версию протокола IP — протокол IPv6, в котором резко расширяется адресное пространство.

Однако и текущая версия протокола IP (IPv4) поддерживает технологии, направленные на более экономное расходование IP-адресов, такие, например, как NAT и CIDR.

Адресация и технология CIDR

Адресация и технология CIDR

Технология бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR) основана на использовании масок для более гибкого распределения адресов и более эффективной маршрутизации.

Она допускает произвольное разделение IP-адреса на поля для нумерации сети и узлов.

При такой системе адресации клиенту может быть выдан пул адресов, более точно соответствующий его запросу, чем это происходит при адресации, основанной на классах адресов.

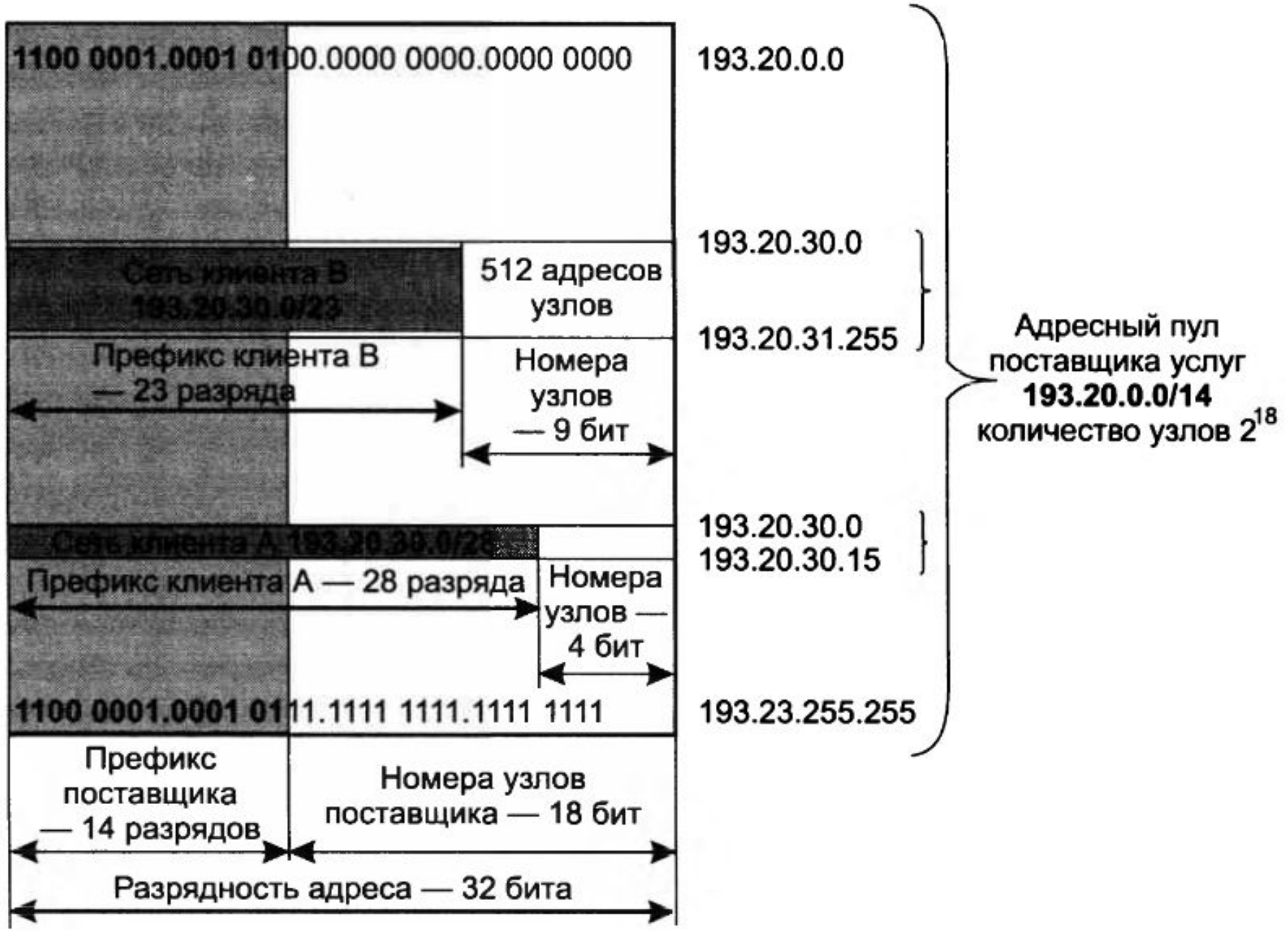
Адресация и технология CIDR

Например, если клиенту А (смотри рисунок на следующем слайде) требуется всего 13 адресов, то вместо выделения ему сети стандартного класса С (класса с наименьшим числом узлов — 256) ему может был назначен пул адресов 193.20.30.0/28.

Эта запись, имеющая вид IP-адрес/маска, интерпретируется следующим образом: «сеть, не принадлежащая ни к какому стандартному классу, номер которой содержится в 28 старших двоичных разрядах IP-адреса 193.20.30.0, имеющая 4-битовое поле для нумерации 16 узлов».

Все это вполне удовлетворяет требованиям клиента А.

Очевидно, что такой вариант намного более экономичен, чем раздача сетей стандартных классов «целиком».


1100 0001.0001 0100.0000 0000.0000 0000
193.20.0.0
193.20.30.0
Сеть клиента B
193.20.30.0/23
512 адресов
узлов
193.20.31.255
Префикс клиента B
— 23 разряда
Номера
узлов
— 9 бит
Адресный пул
поставщика услуг
193.20.0.0/14
количество узлов 2^18
193.20.30.0
Сеть клиента A 193.20.30.0/28
193.20.30.15
Префикс клиента A — 28 разряда
Номера
узлов —
4 бит
1100 0001.0001 0111.1111 1111.1111 1111
193.23.255.255
Префикс
поставщика
— 14 разрядов
Номера узлов
поставщика — 18 бит
Разрядность адреса — 32 бита

Адресация и технология CIDR

Определение пула адресов в виде пары IP-адрес/маска возможно только при выполнении нескольких условий.

Прежде всего адресное пространство, из которого организация, распределяющая адреса, «нарезает» адресные пулы для заказчиков, должно быть **непрерывным**.

При таком условии все адреса имеют общий **префикс** — одинаковую последовательность цифр в старших разрядах адреса.

Непрерывность адресного пространства является очень важным свойством, непосредственно влияющим на эффективность маршрутизации.

Адресация и технология CIDR

Рассмотрим еще один пример.

Пусть клиент В собирается связать в сеть 500 компьютеров.

Вместо того чтобы выделять ему две сети класса С по 256 узлов каждая, клиенту назначают пул адресов в виде пары 193.20.30.0/23.

Эта запись означает, что клиенту выделена сеть неопределенного класса, в которой под нумерацию узлов отведено 9 младших битов, что, как и в случае двух сетей класса С, позволяет адресовать 512 узлов.

Преимущество этого варианта с маской перед вариантом с двумя сетями состоит в том, что в первом случае непрерывность пула адресов гарантирована.

Адресация и технология CIDR

Благодаря CIDR поставщик услуг получает возможность «нарезать» блоки из выделенного ему адресного пространства в соответствии с действительными требованиями каждого клиента.

Технология CIDR помогает не только экономно расходовать адреса, но и более эффективно осуществлять маршрутизацию.

Отображение IP-адресов на локальные адреса

Отображение IP-адресов на локальные адреса

Одной из главных задач, которая ставилась при создании протокола IP, являлось обеспечение совместной согласованной работы в сети, состоящей из подсетей, в общем случае использующих разные сетевые технологии.

При перемещении IP-пакета по составной сети взаимодействие технологии TCP/IP с локальными технологиями подсетей происходит многократно.

На каждом маршрутизаторе протокол IP определяет, какому следующему маршрутизатору в этой сети надо направить пакет.

Отображение IP-адресов на локальные адреса

В результате решения этой задачи протоколу IP становится известен IP-адрес интерфейса следующего маршрутизатора (или конечного узла, если эта сеть является сетью назначения).

Чтобы локальная технология сети смогла доставить пакет следующему маршрутизатору, необходимо:

- упаковать пакет в кадр соответствующего для данной сети формата (например, Ethernet);
- снабдить данный кадр локальным адресом следующего маршрутизатора.

Решением этих задач занимается уровень сетевых интерфейсов стека TCP/IP.

Протокол разрешения адресов

Протокол разрешения адресов

Как уже было сказано, никакой функциональной зависимости между локальным адресом и его IP-адресом не существует, следовательно, единственный способ установления соответствия — **ведение таблиц**.

В результате конфигурирования сети каждый интерфейс «знает» свои IP-адрес и локальный адрес, что можно рассматривать как таблицу, состоящую из одной строки.

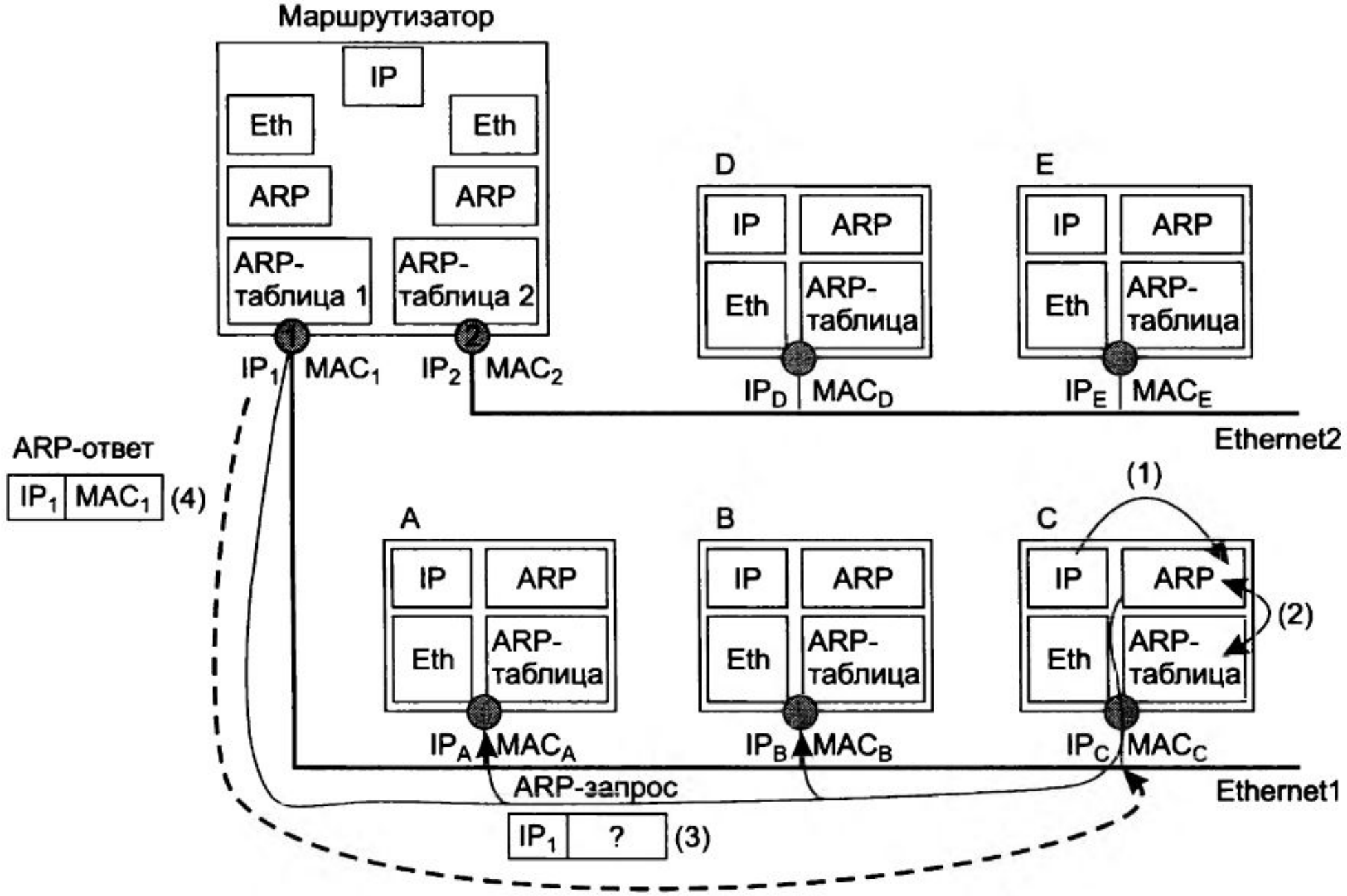
Проблема состоит в том, как организовать обмен имеющейся информацией между узлами сети.

Протокол разрешения адресов

Для определения локального адреса по IP-адресу используется **протокол разрешения адресов** (Address Resolution Protocol, ARP).

Протокол разрешения адресов реализуется различным образом в зависимости от того, работает ли в данной сети протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещания или же какой-либо из протоколов глобальной сети (MPLS, Frame Relay, ATM), которые, как правило, не поддерживают широковещательный доступ.

Рассмотрим работу протокола ARP в локальных сетях с широковещанием.


Маршрутизатор
IP
Eth
Eth
ARP
ARP
ARP-таблица 1
ARP-таблица 2
IP1
MAC1
IP2
MAC2
D
IP
ARP
Eth
ARP-таблица
IPD
MACD
E
IP
ARP
Eth
ARP-таблица
IPE
MACE
Ethernet2
ARP-ответ
IP1
MAC1
(4)
(1)
A
IP
ARP
Eth
ARP-таблица
IPA
MACA
B
IP
ARP
Eth
ARP-таблица
IPB
MACB
C
IP
ARP
Eth
ARP-таблица
(2)
IPC
MACC
ARP-запрос
IP1
?
(3)
Ethernet1

Протокол разрешения адресов

На рисунке показан фрагмент IP-сети, включающий две сети — Ethernet 1 (из трех конечных узлов Л, В и С) и Ethernet 2 (из двух конечных узлов D и Е).

Сети подключены соответственно к интерфейсам 1 и 2 маршрутизатора.

Каждый сетевой интерфейс имеет IP-адрес и MAC-адрес.

Пусть в какой-то момент IP-модуль узла С направляет пакет узлу D.

Протокол IP узла С определил IP-адрес интерфейса следующего маршрутизатора — это IP_1.

Протокол разрешения адресов

Теперь, прежде чем упаковать пакет в кадр Ethernet и направить его маршрутизатору, необходимо определить соответствующий MAC-адрес.

Для решения этой задачи протокол IP обращается к протоколу ARP.

Протокол ARP поддерживает на каждом интерфейсе сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе функционирования сети накапливается информация о соответствии между IP-адресами и MAC-адресами других интерфейсов данной сети.

Первоначально, при включении компьютера или маршрутизатора в сеть, все его ARP-таблицы пусты.

Протокол разрешения адресов

1. На первом шаге происходит передача от протокола IP протоколу ARP примерно такого сообщения: «Какой MAC-адрес имеет интерфейс с адресом IP_1?»

2. Работа протокола ARP начинается с просмотра собственной ARP-таблицы. Предположим, что среди содержащихся в ней записей отсутствует запрашиваемый IP-адрес.

3. В этом случае протокол ARP формирует **ARP-запрос**, вкладывает его в кадр протокола Ethernet и широковещательно рассылает.

Заметим, что зона распространения ARP- запроса ограничивается сетью Ethernet 1, так как на пути широковещательных кадров барьером стоит маршрутизатор.

Протокол разрешения адресов

4. Все интерфейсы сети Ethernet 1 получают ARP-запрос и направляют его «своему» протоколу ARP. ARP сравнивает указанный в запросе адрес IP_1 с IP-адресом собственного интерфейса.

5. Протокол ARP, который констатировал совпадение (в данном случае это ARP интерфейса 1 маршрутизатора), формирует ARP-ответ.

В ARP-ответе маршрутизатор указывает локальный адрес MAC_1 соответствующий адресу IP_1 своего интерфейса, и отправляет его запрашивающему узлу (в данном примере узлу С).

Протокол разрешения адресов

ARP-запросы и ARP-ответы имеют один и тот же формат. В таблице в качестве примера приведены значения полей реального ARP-запроса, переданного по сети Ethernet.

Поле	Значение
Тип сети	1 (0x1)
Тип протокола	2048 (0x800)
Длина локального адреса	6 (0x6)
Длина сетевого адреса	4 (0x4)
Операция	1 (0x1)
Локальный адрес отправителя	008048EB7E60
Сетевой адрес отправителя	194.85.135.75
Локальный (искомый) адрес получателя	000000000000
Сетевой адрес получателя	194.85.135.65

Протокол разрешения адресов

В поле типа сети для сетей Ethernet указывается значение 1.

Поле типа протокола позволяет использовать протокол ARP не только с протоколом IP, но и с другими сетевыми протоколами.

Для IP значение этого поля равно 0x0800.

Длина локального адреса для протокола Ethernet равна 6 байт, а длина IP-адреса — 4 байта.

В поле операции для ARP- запросов указывается значение 1, для ARP-ответов — значение 2.

Из этого запроса видно, что в сети Ethernet узел с IP-адресом 194.85.135.75 пытается определить, какой MAC-адрес имеет другой узел той же сети, сетевой адрес которого 194.85.135.65.

Протокол разрешения адресов

Поле искомого локального адреса **заполнено нулями**.

Ответ присылает узел, опознавший свой IP-адрес.

Если в сети нет машины с искомым IP- адресом, то ARP-ответа не будет.

Протокол IP уничтожает IP-пакеты, направляемые по этому адресу.

В следующей таблице показаны значения полей ARP-ответа, который мог бы поступить на приведенный ARP-запрос.

Протокол разрешения адресов

Поле	Значение
Тип сети	1 (0x1)
Тип протокола	2048 (0x800)
Длина локального адреса	6 (0x6)
Длина сетевого адреса	4 (0x4)
Операция	2 (0x1)
Локальный адрес отправителя	00E0F77F1920
Сетевой адрес отправителя	194.85.135.65
Локальный (искомый) адрес получателя	008048EB7E60
Сетевой адрес получателя	194.85.135.75

Протокол разрешения адресов

В результате обмена ARP-сообщениями модуль IP, пославший запрос с интерфейса, имеющего адрес 194.85.135.75, определил, что IP-адресу 194.85.135.65 соответствует MAC-адрес 00E0F77F1920.

Этот адрес затем помещается в заголовок кадра Ethernet, ожидавшего отправления IP-пакета.

Чтобы уменьшить число ARP-обращений в сети, найденное соответствие между IP-адресом и MAC-адресом сохраняется в ARP-таблице соответствующего интерфейса, в данном случае — это запись:

194.85.135.65 - 00E0F77F1920

Протокол разрешения адресов

Данная запись в ARP-таблице появляется автоматически, спустя несколько миллисекунд после того, как модуль ARP проанализирует ARP-ответ.

Теперь, если вдруг вновь возникнет необходимость послать пакет по адресу 194.85.135.65, то протокол IP, прежде чем посылать широковещательный запрос, проверит, нет ли уже такого адреса в ARP-таблице.

ARP-таблица пополняется **не только** за счет **поступающих** на данный интерфейс **ARP-ответов**, но и в результате извлечения полезной информации из широковещательных ARP- запросов.

Протокол разрешения адресов

Действительно, в каждом запросе, как это видно из таблиц, содержатся IP- и MAC-адрес отправителя.

Все интерфейсы, получившие этот запрос, могут поместить информацию о соответствии локального и сетевого адресов отправителя в собственную ARP-таблицу.

В частности, все узлы, получившие ARP-запрос, могут по полнить свою ARP-таблицу записью:

194.85.135.75 - 008048EB7E60

Протокол разрешения адресов

Таким образом, вид ARP-таблицы, в которую в ходе работы сети были добавлены две упомянутые нами записи, иллюстрирует следующая таблица.

IP-адрес	MAC-адрес	Тип записи
194.85.135.65	00E0F77F1920	Динамический
194.85.135.75	008048EB7E60	Динамический
194.85.60.21	008048EB7567	Статический

В ARP-таблицах существуют два типа записей:

- динамические,
- статические.

Протокол разрешения адресов

Статические записи создаются вручную с помощью утилиты ARP и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор остается включенным.

Динамические записи должны периодически обновляться.

Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы.

Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях.

Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют **ARP-кэшем**.

Протокол разрешения адресов

Некоторые реализации протоколов IP и ARP не ставят IP-пакеты в очередь на время ожидания ARP-ответов.

Вместо этого IP-пакет просто уничтожается, а его восстановление возлагается на модуль TCP или прикладной процесс, работающий через протокол UDP.

Такое восстановление выполняется за счет тайм-аутов и повторных передач.

Успешность повторной передачи обеспечивается первой по пыткой, которая вызывает заполнение ARP-таблицы.

Протокол разрешения адресов

Совсем другой способ разрешения адресов используется в **глобальных сетях**, в которых не поддерживается широковещательная рассылка.

Здесь администратору сети чаще всего приходится вручную формировать и помещать на какой-либо сервер ARP-таблицы, в которых он задает, например, соответствие IP-адресов адресам X.25, имеющих для протокола IP смысл локальных адресов.

В то же время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях.

Для этой цели среди всех маршрутизаторов, подключенных к какой-либо глобальной сети, выделяется специальный маршрутизатор, который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети.

Протокол разрешения адресов

При таком централизованном подходе вручную нужно задать для всех узлов и маршрутизаторов только IP-адрес и локальный адрес выделенного для этих целей маршрутизатора.

При включении каждый узел и маршрутизатор регистрируют свой адрес в выделенном маршрутизаторе.

Всякий раз, когда возникает необходимость определения по IP-адресу локального адреса, модуль ARP обращается к выделенному маршрутизатору с запросом и автоматически получает ответ без участия администратора.

Работающий таким образом маршрутизатор называют **ARP-сервером**.

Протокол разрешения адресов

В некоторых случаях возникает обратная задача — нахождение IP-адреса по известному локальному адресу.

Тогда в действие вступает реверсивный протокол разрешения адресов (Reverse Address Resolution Protocol, RARP).

Этот протокол используется, например, при старте бездисковых станций, не знающих в начальный момент времени своего IP-адреса, но знающих MAC-адрес своего сетевого адаптера.

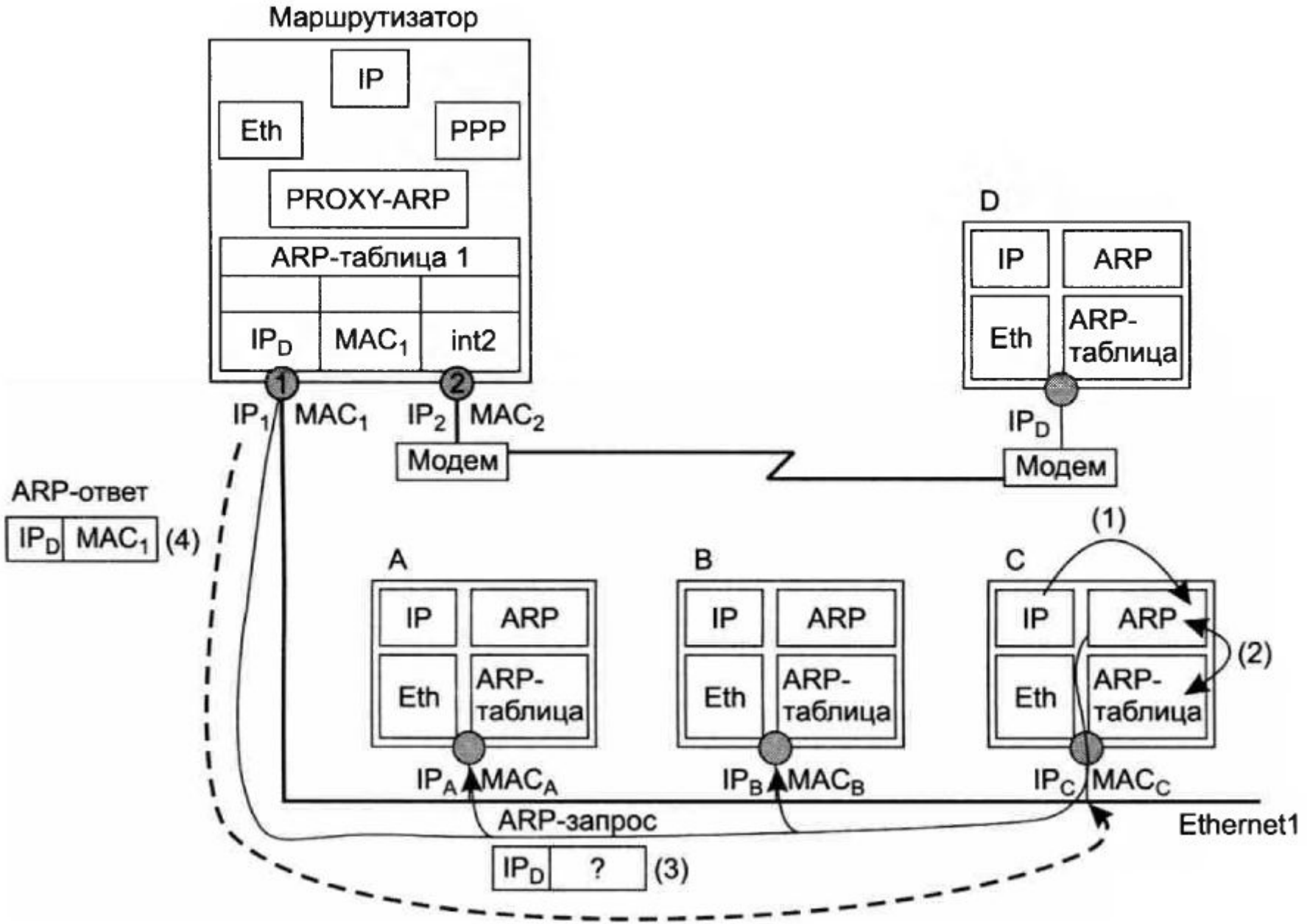
Протокол Proxy-ARP

Протокол Proxy-ARP

Протокол Proxy-ARP — это одна из разновидностей протокола ARP, позволяющая отображать IP-адреса на аппаратные адреса в сетях, поддерживающих широковещание, даже в тех случаях, когда искомый узел находится за пределами данного домена коллизий.

На следующем рисунке показана сеть, один из конечных узлов которой (компьютер D) работает ***в режиме удаленного узла***.

В этом режиме узел обладает всеми возможностями компьютеров основной части сети Ethernet, в частности он имеет IP-адрес (IP_D), относящийся к той же сети.


Маршрутизатор
IP
Eth
PPP
PROXY-ARP
ARP-таблица 1
IP_D
MAC_1
int2
1
2
IP_1
MAC_1
IP_2
MAC_2
Модем
D
IP
ARP
Eth
ARP-таблица
IP_D
Модем
ARP-ответ
IP_D
MAC_1
(4)
(1)
A
B
C
IP
ARP
Eth
ARP-таблица
(2)
IP_A
MAC_A
IP_B
MAC_B
IP_C
MAC_C
ARP-запрос
Ethernet1
IP_D
?
(3)

Протокол Proxy-ARP

Для всех конечных узлов сети Ethernet особенности подключения удаленного узла (наличие модемов, коммутируемая связь, протокол PPP) абсолютно прозрачны — они взаимодействуют с ним обычным образом.

Чтобы такой режим взаимодействия стал возможным, среди прочего необходим протокол Proxy-ARP.

Поскольку удаленный узел подключен к сети по протоколу PPP, то он, очевидно, ***не имеет MAC-адреса***.

Протокол Proxy-ARP

Пусть приложение, работающее, например, на компьютере C, решает послать пакет компьютеру D.

Ему известен IP-адрес узла назначения (IP_D), однако, как мы уже не раз отмечали, для передачи пакета по сети Ethernet его необходимо упаковать в кадр Ethernet и снабдить MAC-адресом.

Для определения MAC-адреса IP-протокол узла C обращается к протоколу ARP, который посылает широковещательное сообщение с ARP-запросом.

Если бы в этой сети на маршрутизаторе не был установлен протокол Proxy-ARP, на этот запрос не откликнулся бы ни один узел.

Протокол Proxy-ARP

Однако протокол Proxy-ARP установлен на маршрутизаторе и работает следующим образом.

При подключении к сети удаленного узла D в таблицу ARP-маршрутизатора заносится запись

$$IP_D — MAC_1 — int2$$

Эта запись означает, что:

- при поступлении ARP-запроса на маршрутизатор относительно адреса IP_D в ARP- ответ будет помещен аппаратный адрес MAC_1 соответствующий аппаратному адресу интерфейса 1 маршрутизатора;
- узел, имеющий адрес IP_D, подключен к интерфейсу 2 маршрутизатора.

Протокол Proxy-ARP

В ответ на посланный узлом C широковещательный ARP-запрос откликается маршрутизатор с установленным протоколом Proxy-ARP.

Он посылает «ложный» ARP-ответ, в котором на место аппаратного адреса компьютера D помещает собственный адрес MAC_1.

Узел C, не подозревая «подвоха», посылает кадр с IP-пакетом по адресу MAC_1.

Протокол Proxy-ARP

Получив кадр, маршрутизатор с установленным протоколом Proxy-ARP «понимает», что он направлен не ему (в пакете указан чужой IP-адрес) и поэтому надо искать адресата в ARP-таблице.

Из таблицы видно, что кадр надо направить узлу, подключенному ко второму интерфейсу.

Это лишь простейшая схема применения протокола Proxy-ARP.

Тем не менее, она достаточно полно отражает логику работы этого протокола.

Контрольные вопросы

1. Назовите

Список литературы:

1. Беленькая М. Н., Малиновский С. Т., Яковенко Н. В. Администрирование в информационных системах. Учебное пособие. - Москва, Горячая линия - Телеком, 2011.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.

Список ссылок:

http://polpoz.ru/umot/lokalenaya-sete-ooo-nadejnij-kontakt/10.png

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru