Лекция6.Протокол ARP, класс и маска IP адресов

Для передачи информации между двумя хостами в сети необходимо знать четыре адреса:

- Destination MAC address
- Source MAC address
- Destination IP address
- Source IP address

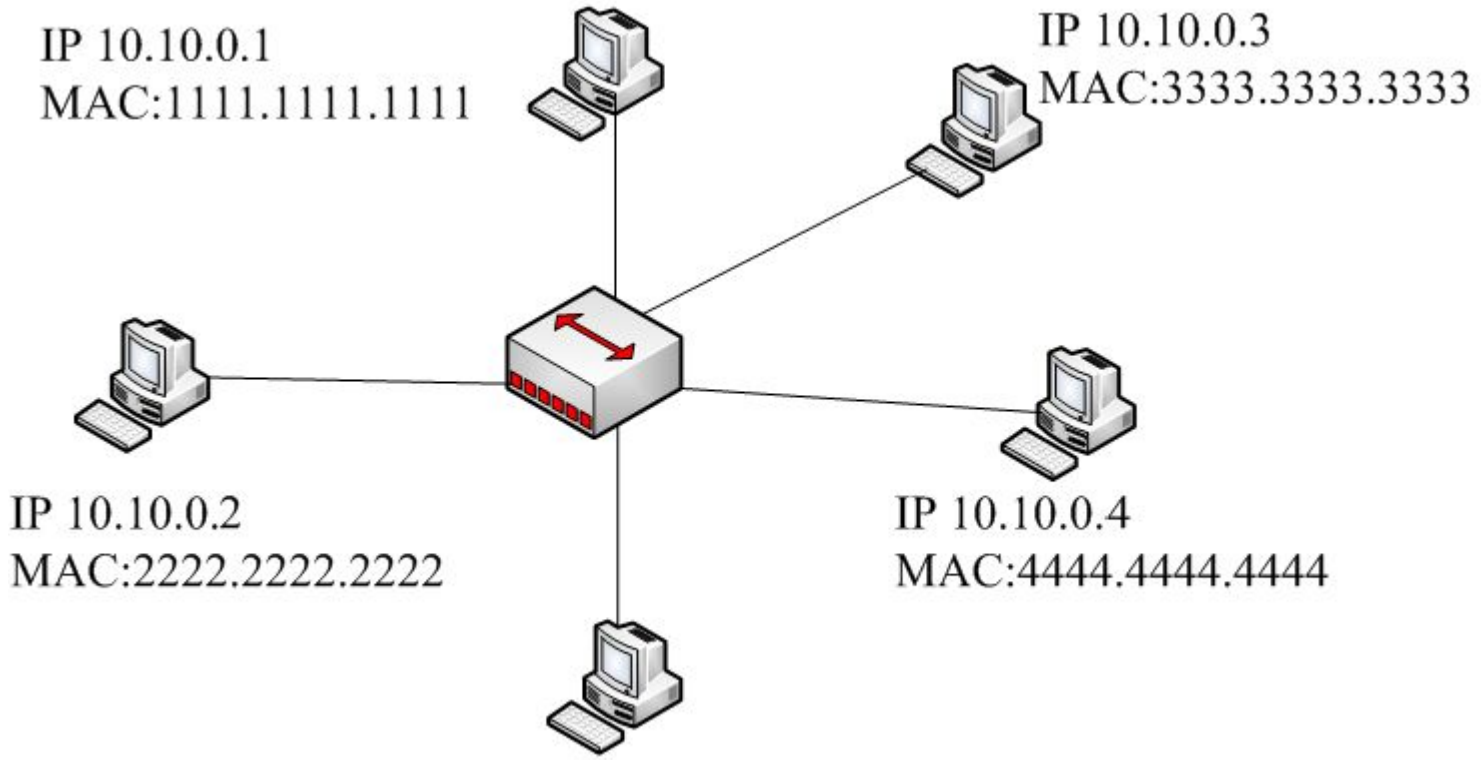
Не зная хотя бы один из этих адресов, информацию передать будет невозможно.

На канальном уровне сетевая карта всегда знает свой адрес (MAC адрес источника), если сетевая карта не знает своего MAC адреса, значит, она имеет явные неисправности и работа такой сетевой карты в сети не будет нормальной.

Свой IP адрес (адрес источника) задаётся в настройках операционной системы, его можно менять и он не «прикреплён» к сетевой карте как MAC адрес. Этот параметр устанавливается пользователем и поэтому также доступен.

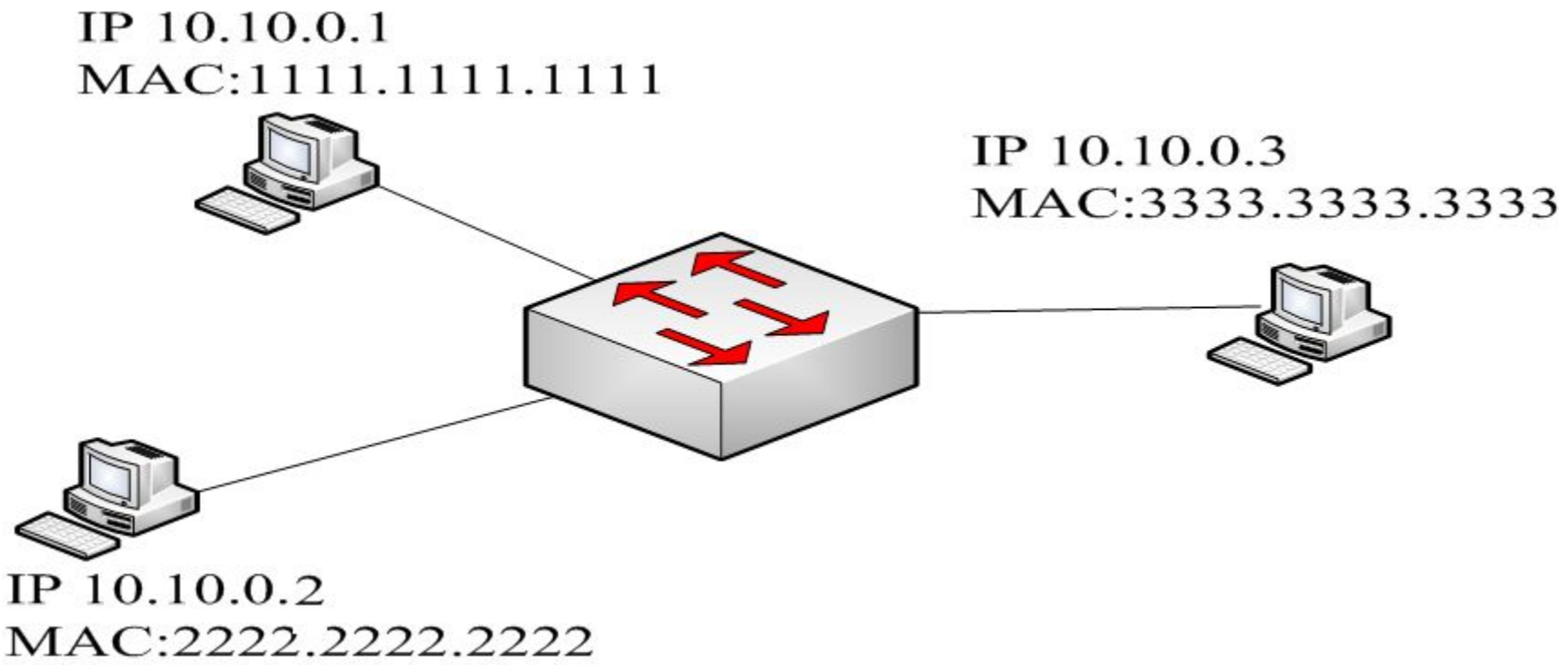
IP адрес удалённого устройства либо задаётся в явном виде (указывается в команде на формирование пакетов, к этому узлу, например, ping 192.168.0.1), либо в неявном, например посредством службы доменных имён или таблицы хостов. Адрес, который задан неявно всё равно будет транслирован в стандартный IP адрес и передан обратно станции отправителю для формирования пакетов. Итак, IP адрес назначения также задаётся пользователем.

Рассмотрим такую топологию, где центральным звеном является концентратор.



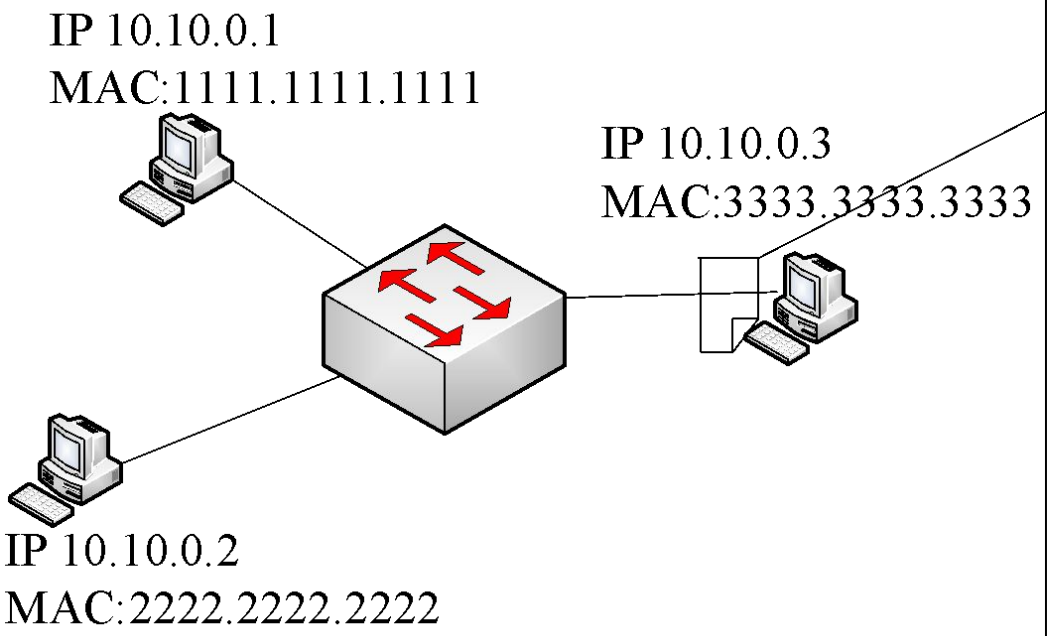
А как узнать MAC адрес назначения? Ведь без него не получится сформировать из пакета фрейм и отправить в сеть. Для этого был создан протокол Address Resolution Protocol (ARP), целью которого является раскрытия MAC адреса определённого устройства по IP адресу этого устройства. Каждое «разумное» устройство в сети составляет так называемые ARP таблицы, в которых указаны пары IP и MAC адресов для создания фреймов, зная сетевой адрес назначения.

Теперь рассмотрим случай, когда в сегменте находится несколько доменов коллизии.



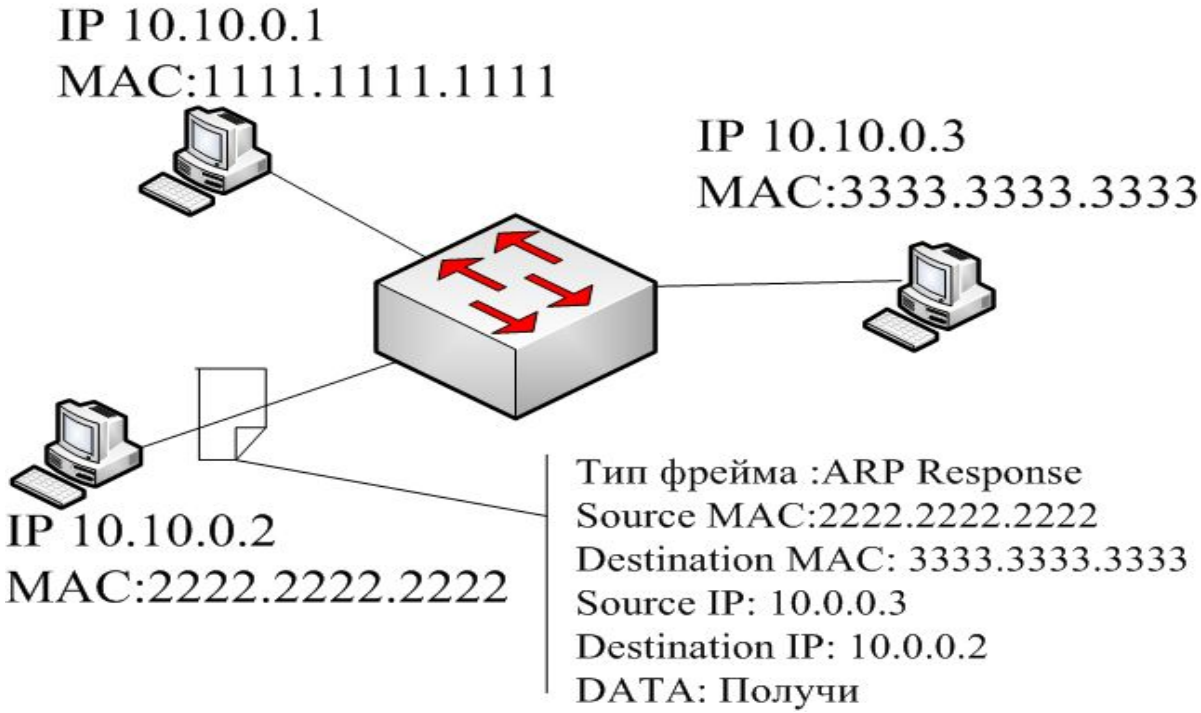
Из-за того, что центром топологии является коммутатор, а не концентратор, как в предыдущем случае, каждая станция находится в своём домене коллизии. Коммутатор не передаёт фреймы, которые адресованы одной станции на все порты, вместо этого он смотрит в таблицу коммутации и точно определяет на какой порт необходимо отправить фрейм, чтобы он дошёл до нужной станции. В связи с этим, заполнение ARP таблиц, как было описано в предыдущем случае невозможно.

В том случае, если станция хочет отправить фрейм другой станции, но она не знает MAC адрес назначения, ей необходимо отправить специальный фрейм, который называется ARP Request (ARP запрос).



Тип фрейма :
ARP Request
Source
MAC:3333.3333.3333
Destination MAC:
FFFF.FFFF.FFFF
Source IP: 10.0.0.3
Destination IP: 10.0.0.2
DATA: Скажи свой
MAC

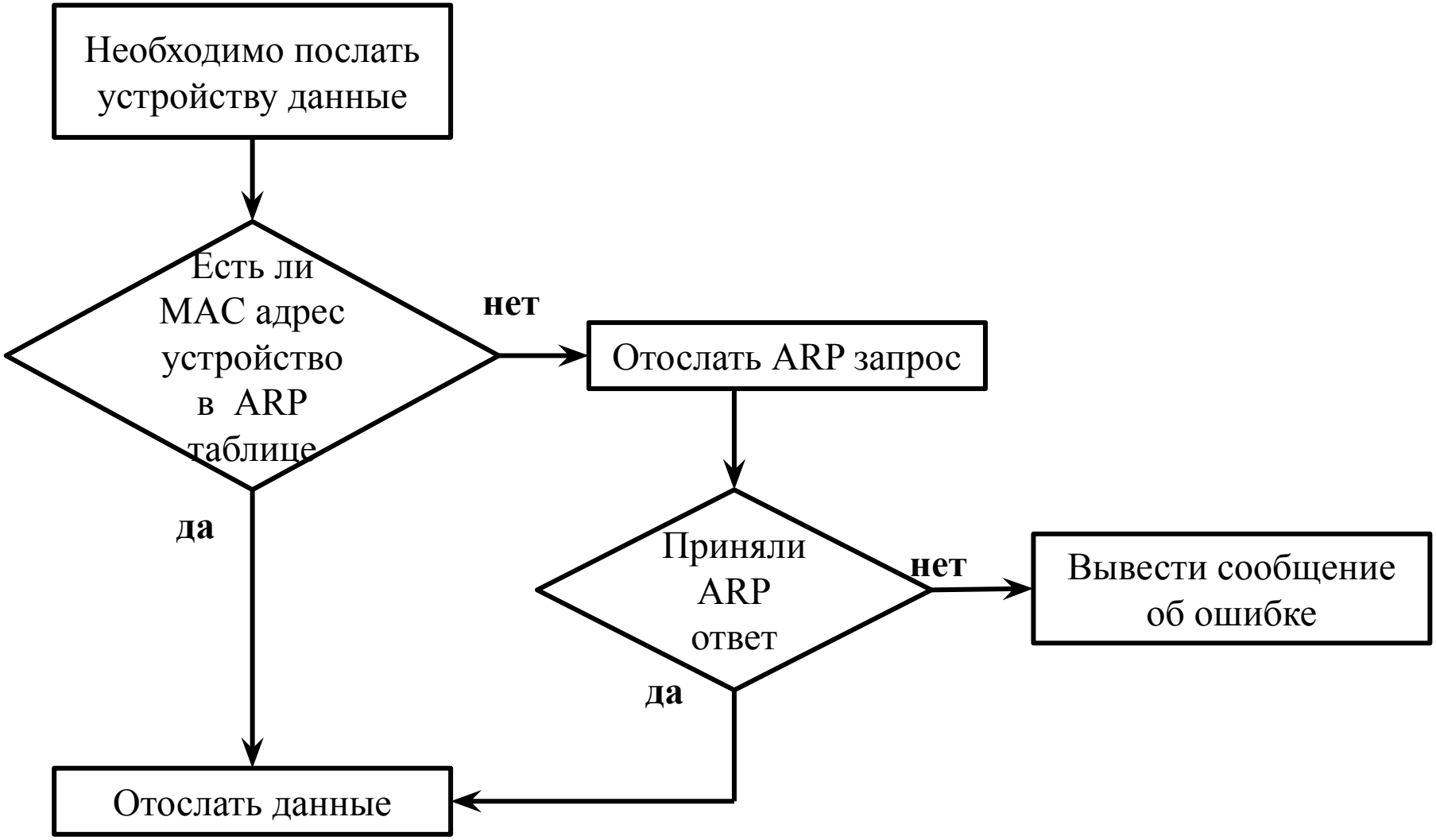
После отправки фрейма станцией, его получит коммутатор, он посмотрит в поле MAC адреса назначения и увидев там широковещательный адрес разошлёт этот фрейм на все порты кроме порта источника. Обе станции в топологии получат этот фрейм, обе раскроют фрейм, так как он адресован всем, а вот на сетевом уровне на этот пакет ответит только та станция, IP адрес которой совпадает с IP адресом, который указан в пакете в поле назначения.



Когда станция получит ARP ответ, она дополнит свою ARP таблицу и может теперь отправлять фреймы.

ARP Table	
IP Address	**MAC Address**
10.0.0.2	**2222.2222.2222**

Алгоритм отправки фреймов сетевых устройств



Формы записи IP-адреса. IP-адрес имеет длину 4 байта (32 бита) и состоит из двух логических частей – номера сети и номера узла в сети. Наиболее употребляемой формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например: 126.10.2.30. Этот же адрес может быть представлен в двоичном формате: 01111110 00001010 00000010 00011110.

А также в шестнадцатеричном формате:7F.0A.02.1D.

Классы IP-адресов. Традиционная схема деления IP-адреса на номер сети и номер узла основана на понятии класса, который определяется значениями нескольких первых битов адреса. Именно потому, что первый байт адреса 185.23.44.206 попадает в диапазон 128-191, мы можем сказать, что этот адрес относится к классу B, а значит, номером сети являются первые два байта IP-адреса, дополненные двумя нулевыми байтами – 185.23,0.0, а номером узла – два младшие байта, дополненные с начала двумя нулевыми байтами – 0.0.44.206.

Класс	**Первые биты**	**Наименьший номер сети**	**Наибольший номер сети**	**Максимальное число узлов в сети**
A	**0**	**1.0.0.0**	**126.0.0.0**	**2^{24}**
B	**10**	**128.0.0.0**	**191.255.0.0**	**2^{16}**
C	**110**	**192.0.1.0**	**223.255.255.0**	**2^{8}**
D	**1110**	**224.0.0.0**	**239.255.255.255**	**Multicast**
E	**11110**	**240.0.0.0**	**247.255.255.255**	**Зарезервирован**

IP – адресация 6 версии

3	13	8	24	16	64
FP	TLA	RESERV	NLA	SLA	ID Inerface

Префикс формата (Format Prefix, FP) для этого типа адресов имеет размер три бита и значение 001.

Следующие три поля — агрегирования верхнего (Top-Level Aggregation, TLA), следующего (Next-Level Aggregation, NLA) и местного (Site-Level Aggregation, SLA) уровней — описывают три уровня идентификации сетей.

Поле TLA предназначено для идентификации сетей самых крупных поставщиков услуг. Конкретное значение этого поля представляет собой общую часть адресов, которыми располагает данный поставщик услуг. Сравнительно небольшое количество разрядов, отведенных под это поле (13), выбрано специально для ограничения размера таблиц маршрутизации в магистральных маршрутизаторах самого верхнего уровня Интернета. Это поле позволяет перенумеровать 8196 сетей поставщиков услуг верхнего уровня, а значит, число записей, описывающих маршруты между этими сетями, также будет ограничено значением 8196, что ускорит работу магистральных маршрутизаторов. Следующие 8 разрядов зарезервированы на будущее для расширения при необходимости поля TLA.

Поле NLA предназначено для нумерации сетей средних и мелких поставщиков услуг. Значительный размер поля NLA позволяет путем агрегирования адресов отразить многоуровневую иерархию поставщиков услуг.

Поле SLA предназначено для адресации подсетей отдельного абонента, например подсетей одной корпоративной сети. Предполагается, что поставщик услуг назначает некоторому предприятию номер его сети, состоящий из фиксированного значения полей TLA и NLA, которые в совокупности являются аналогом номера сети версии IPv4. Остальная часть адреса — поля SLA и идентификатор интерфейса — поступает в распоряжение администратора корпоративной сети, который полностью берет на себя формирование адреса и не должен согласовывать этот процесс с поставщиком услуг. Причем поле идентификатора интерфейса имеет вполне определенное назначение — оно должно хранить физический адрес узла. На этом уровне также можно агрегировать адреса небольших подсетей в более крупные подсети, и размер поля SLA в 16 бит обеспечивает достаточную свободу и гибкость построения внутрикорпоративной иерархии адресов.

Идентификатор интерфейса является аналогом номера узла в IPv4. Отличием версии IPv6 является то, что в общем случае идентификатор интерфейса просто *совпадает с его локальным (аппаратным) адресом*, а не представляет собой произвольно назначенный администратором номер узла. Идентификатор интерфейса имеет длину 64 бита, что позволяет поместить туда MAC-адрес (48 бит), адрес X.25 (до 60 бит), адрес конечного узла ATM (48 бит

Протокол ICMP
ICMP Делится на два класса
1. Диагностические сообщения об ошибках
2. информационные сообщения типа запрос/ответ

ICMP-сообщение инкапсулируется в поле данных IP-пакета

Инкапсуляция и формат ICMP-сообщения

Тип содержит код, определяющий тип сообщения. Показан в таблице.
Код более тонко дифференцирует тип обшики.

Возможные значение поля типа

значение	Тип сообщения
0	Эхо ответ
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправление маршрута
8	Эхо-запрос

Коды, детализирующие причину ошибки о недостижимости узла назначения

код	причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
6	Сеть назначения неизвестна

Формат ICMP-сообщений тип эхо-запрос/это-ответ

Формат ICMP-сообщений об ошибке — недостижимости узла назначения