Приблизительный план практических занятий

1. Особенности стандартизации и адресации всемирной паутины (WEB). Протокол сетевого уровня IPv4, классы сетей и IPадресация.

2. Переход к системе нумерации IPv6. Особенности протокола TCP/IP. Протоколы IPмаршрутизации RIP, OSPF.

3. Особенности сигнализации на прикладном уровне ISUPОКС 7 на примере реализации ДВО ISDNзавершения установления соединения к занятому абоненту (CCBS – Call Completion To Busy Subscriber).

4. Классы протокола подсистемы транзакционных возможностей. Примеры реализации процедур подуровней компонент и транзакций.

5. Реализация процедур ремаршрутизации сигнального трафика на уровне МТР 3 ОКС 7 при отказе на примере сети Гостехнопарка ЛОНИИС.

6. Примеры успешных и неуспешных установлений соединений SCCPОКС 7 (класс 2).

Стандарты в сфере Интернет

Список сокращений:

CERT (ComputerEmergencyResponseTeam) – центркруглосуточного реагирования на инциденты информационной безопасности.

IAB (InternetArchitectureBoard) – советпоархитектуреИнтернет.

IETF (InternetEngineeringTaskForce) – специальнаярабочаягруппапопланированию Интернет.

IESG (InternetEngineeringSteeringGroup) – группа по выработке инженерного регламента Интернет.

IRTF(InternetResearchTaskForce) – рабочая группа исследования Интернет.

ICANN (InternetCorporationforAssignedNamesandNumber) – международная организация по распределению доменных имен и IPадресов.

Интернет самая необычная из всех сетей. Практически любой объект можно подключить к Интернет, чтобы предложить ресурсы, или для доступа к ним.По Интернет может гулять любой вид информации без каких-либо ограничений. Отсутствует центральный орган, который регулировал бы работу сети Интернет, хотя существуют организации, устанавливающие определенные фундаментальные принципы и руководящие работой сети.

Существует ряд организаций, участвующих в различных мероприятиях по администрированию и поддержке Интернет. В контексте данной книги, среди этих организаций следует упомянуть CERT, IAB, IETF, IESG, IRTF, ICANNи «The InternetSociety» (Общество Интернет известное как ISOC). Далее, кратко опишем каждую из приведенных выше организаций.

Группа реагирования на нарушения компьютерной защиты (CERT)–группа экспертов Университета Корнеги-Меллона, которая отвечает на вопросы, связанные с нарушением компьютерной защиты в сети Интернет. CERTбыла образована ARPAв ноябре 1998 года как реакция на ряд инцидентов, связанных с появлением вирусных программ самотиражирования.

Совет по архитектуре IAB, первоначально – Координационный Совет по сети Интернет – добровольный орган, имеющий в своем составе 12 экспертов, которые используют ресурсы своих компаний-спонсоров для того, чтобы способствовать интересам Интернет. IAB контролирует и координирует деятельность двух проблемных (рабочих) групп: IETFиIRTF. В

совокупности,эти организации вырабатывают техническую политику и направления работы.

*Инженерная проблемная группа Интернет (IETF)*определяет, устанавливает приоритеты и вырабатывает решения по краткосрочным вопросам и проблемам, включая протоколы, архитектуру и эксплуатацию. Предложенные стандарты публикуются в Интернет в виде запросов комментариев и предложений (RFC). После выработки окончательной версии стандарта, он поступает на утверждение в группу управления инженеров Интернет (IESG).

Научно-исследовательская проблемная группа Интернет (IRTF) занимается долгосрочными вопросами, включая схемы адресации и технологии.

Корпорация Интернет по присвоению имен и номеров (ICANN) –некоммерческая организация, образованная в 1999 году. ICANNбыла создана для того, чтобы взять на себя полномочия федерального органа IANAпо распределению общеизвестных номеров портов, управлению IP адресами и присвоению имен доменов. Номера портов представляют собой 16-и битовые величины в диапазоне от 0 до 65536. Общеизвестные порты нумеруются числами в диапазоне от 0 до 1023 и используются системными процессами или прикладными программами. Примерами общеизвестных портов являются: порт 25 для протокола SMTP (простого протокола пересылки почты), порт 80 для протокола HTTP (гипертекстового транспортного протокола) и порт 107 для дистанционной службы Telnet. В среде клиент/сервер

Интернет на базе протокола TCP/IP, сервер назначает порты с учетом протокола прикладного уровня, который выполняется на клиентском уровне. ICANNтакже присваивает IPадреса организациям, желающим поместить компьютеры в Интернет; количество адресов зависит от размеров организации.

Общество Интернет (ISOC) – добровольная организация, которая представляет собой некоторую формальную структуру для администрирования Интернет. Общество Интернет предоставило официальные полномочия IESGпринимать решения по стандартам.

Адресация

Интернет – это совокупность тысяч компьютеров, объединенных в сети, которые, в свою очередь, соединены между собой посредством маршрутизаторов. Для организации линий связи используются все возможные технологии – от коммутируемых телефонных соединений до самых современных оптических систем передачи. Активно используются и спутниковые линии связи.

Сеть Интернет имеет иерархическую структуру. Этот подход является эффективным потому, что позволяет идентифицировать компоненты Интернет посредством адресов, также имеющих иерархическую структуру. Например, в телефонной сети полный номер абонента содержит такие составляющие как код страны, код

междугородней зоны, кодсети, номер АТСТФОП, номер абонента АТС.Аналогичная концепция была принята и в сети Интернет: старшие биты адреса идентифицируют сеть, в которой находится рабочая станция, а младшие – расположение рабочей станции вэтой сети.

Подавляющее большинство сетей сейчас использует протокол IPv4 (интернет – протокол версии 4), хотя уже разработана шестая версия протокола IP, которая применяется в некоторых недавно созданных крупных сетях. Схема адресации протокола IPv4, который был определен в RFC 791, предусматривает размер адресного поля 32 бита, что дает 2^{32} (или 4 294 967 296) потенциальных адресов.

IPадрес любой рабочей станции состоит из *адреса сети* и *адреса компьютера в этой сети.*В архитектуре адресации предусмотрено пять форматов адреса, каждый из которых начинается с одного, двух, трех или четырех битов, идентифицирующих класс сети (класс A, B, C, Dили E). Область сетевого идентификатора (NetworkID) определяет конкретную сеть в классе, а область HostID идентифицирует конкретный компьютер в сети.

- *Адреса класса A*идентифицируются начальным битом 0. Следующие *семь битов* определяют конкретную сеть (число возможных значений – 128 и 2^7). Остальные 24 бита определяют конкретный компьютер в сети, при возможном количестве компьютеров 16 777 216 (2^{24}). Адреса класса Апредназначены для очень крупных сетей с большим количеством рабочих станций. Первые адреса класса

Абыли присвоены таким компаниям как IBMCorporation, Hewlett-PackardCompany, FordMotorCompanyи др.

- *Адреса класса B* идентифицируются начальной двухбитовой двоичной последовательностью 10.Следующие*14 битов* определяют сеть, при возможном количестве сетей 16384 (2^{14}). Остальные *16 битов* определяют конкретный компьютер, с возможным количеством компьютеров – 65536 (2^{16}).
- *Адреса класса C* идентифицируются начальной трехбитовой последовательностью 110.Следующие 21 бит определяют сеть, с возможным количеством сетей – 2 097 152. Остальные *8 битов*определяют конкретный компьютер в сети, с возможным количеством компьютеров 256 (2^8). Большинство организаций имеют адреса класса C.
- *Адреса класса D*идентифицируются начальной четырехбитовой последовательностью 1110. Адреса этого класса предназначены для групповой передачи, а оставшиеся *28 бит* определяют групповой адрес.
- *Адреса класса E*идентифицируются начальной четырехбитовой последовательностью 1110. Адреса этого класса зарезервированы для будущего использования.

Способ, с помощью которого записываются все IPадреса, называется пунктирной десятичной системой обозначений. Каждое 32-битовое адресное поле разделено на *четыре поля*в виде xxx.xxx.xxx.xxx, и каждому полю дается

десятичное числовое значение от 0 до 255, выраженное в виде одного октета ($2^8 = 256$ или $0 \div 255$).

Адреса класса Аначинаются с *1 ÷ 127,адреса класса* В*128 ÷ 191*, и *адреса класса С*–с *192 ÷ 223.* На нижеследующем рисунке,типы IPадресов представлены в более удобной для восприятия графической форме.

Принципы IPадресации

Например, имеется сетькласса В 172.21.2.123/*25*.

Маска подсети 255.255.255.128

Количество подсетей $2^9 = 512$ (9 битов степени числа 2 соответствует адресному пространству, выделенному для узлов сети, перекрывающееся с маской сети, т.е. 25-16 бит)

Количество хостов в каждой сети $2^7 – 2 = 126$ (степень числа 2 равняется 7, а именно, разности 32 – *25* бит).

Далее,исходя из приведенных выше вычислений реализуется разделение на подсети.

Подсеть 0 *172.21.0.0* ÷ 172.21.0.127;

Подсеть 1*172.21.0.128* ÷ 172.21.0.255;

Подсеть 2*172.21.1.0*÷ 172.21.1.127;

Подсеть 3 *172.21.1.128* ÷ 172.21.1.255;

…….

Подсеть 510*172.21.255.0* ÷ 172.21.255.127;

Подсеть 511*172.21.255.128* ÷ 172.21.255.255;

Адреса класса A

	Адрес сети	Адрес компьютера в сети
0	7 битов	24 бита

Адреса класса B

		Адрес сети	Адрес компьютера в сети
1	0	14 битов	16 битов

Адреса класса C

			Адрес сети	Адрес компьютера в сети
1	1	0	21 бит	8 битов

Адреса класса D

				Групповой адрес
1	1	1	0	28 битов

Адреса класса E (резервируются для будущего использования)

1	1	1	1	

Типы IPадресов

Как отмечалось выше, *корпорация Интернет по присвоению имен и номеров (ICANN)* присваивает IP адреса организациям, желающим подключить компьютеры к сети Интернет. Класс IPадреса и, следовательно, количество возможных адресов компьютеров зависит от размеров организации. Организация, которой присвоены номера, может затем переназначить их на основе либо *статической*, либо *динамической адресации.*

Статическая адресация означает жесткую привязку IPадреса к конкретному компьютеру. При динамической адресации компьютеру присваивается доступный IPадрес всякий раз при установлении соединения.Например, поставщик услуг Интернет может иметь один или несколько адресных блоков класса С. При ограниченном количестве доступных IPадресов поставщик присваивает IPадрес компьютеру пользователя всякий раз, когда пользователь коммутируемой линии получает к нему доступ, чтобы установить соединение с Интернет. После завершения соединения, этот IPадрес может присваиваться другим пользователям. Динамическое присвоение IPадресов обычно осуществляется через маршрутизатор, работающий по протоколу DHCP (протокол динамической конфигурации рабочей станции). Наоборот, если доступ к поставщику осуществляется по xDSL, поставщик услуг Интернет обычно присваивает пользователю один или более статических IP адресов. Так как соединение по xDSL всегда активизировано, динамическая адресация для этой категории пользователей неприемлима.

Как уже отмечалось, протокол IPверсии 4 предусматривает размер адресного поля 32 бита, что дает 2^{32} (или 4 294 967 296) потенциальных адресов. Однако, возрастающая популярность технологии TCP/IPпривела к истощению плана нумерации протокола IPv4. Дополнительной проблемой является тот факт, что очень большое количество адресов класса Аи класса Вбыло выделено крупным организациям, которые в действительности в них не нуждались.В связи с тем, что фактически использовался только небольшой процент адресов, огромное количество доступных адресов было потеряно.

Для того, чтобы частично решить данную проблему, комитет IETFв начале 90-х годов опубликовал в документах RFC 1518 и RFC 1519положение о *бесклассовой междоменной маршрутизации (CIDR).*Технология CIDR построена на концепции суперсети (supernetting), состоящей из группы подсетей, каждой из которых присваивается адрес подсети. Но в целом совокупность подсетей выглядит как единая сеть с одним префиксом (например, для Европы выделены префиксы 194 и 195). Благодаря технологии CIDR, сокращается число маршрутов и, следовательно, размер и сложность таблиц маршрутизации, которые должны поддерживать коммутаторы и маршрутизаторы.

Таким образом,компьютер подключенный к сети Интернет, кроме IPадреса может идентифицироваться доменным именем. Сеть Интернет разделена на логические области (домены). Адреса в системе имен доменов (DNS –

DomainNameSystem), администрирование которых лежит на ICANN, имеют стандартный вид, представляющий собой последовательность имен, разделенных точками, например: компьютер.организация.домен. Подавляющее большинство из 45 миллионов (или около того) зарегистрированных доменов верхнего уровня (TLD) является коммерческими. Домены TLD, которые идентифицируются как суффикс доменного имени, бывают двух типов: обобщенные домены верхнего уровня (net, com, org) и коды стран (ru, fi, ua).

ICANN получил от IANAполномочия по администрированию Интернет-адресов.При администрировании со стороны IANA, ответственность за присвоение Имен Доменов Верхнего уровня возлагается на центр сетевой информации Интернет (InterNIC) компании NetworkSolutionsInc.В течение первых десятков лет существования Интернет, присвоение доменов было бесплатным. Позже, InterNic начал брать плату за домены .comв размере $ 70 за первые два года и $ 35 за каждый следующий год. В 1999 году InterNic потерял монопольное право на присвоение доменов, так как в апреле 1999 года были утверждены четыре конкурентные организации на испытательный срок до 25 июня 1999 года. ICANNтакже объявил, что ряд других заявителей удовлетворяют его критериям аккредитации, и они будут аккредитованы по окончании испытательного срока.

Имена доменов гораздо легче запомнить и ввести, но необходимопроизводить их преобразование для перевода имен доменов в IPадреса; это необходимо для того, чтобы

разные маршрутизаторы и коммутаторы могли направить информацию в нужный пункт назначения.

Протокол IPверсии 4

В качестве основного протокола сетевого уровня в стеке протоколов TCP/IPиспользуется протокол IP, который изначально проектировался как протокол передачи пакетов в сетях, состоящих из большого количества локальных сетей. Поэтому протокол IPхорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи.

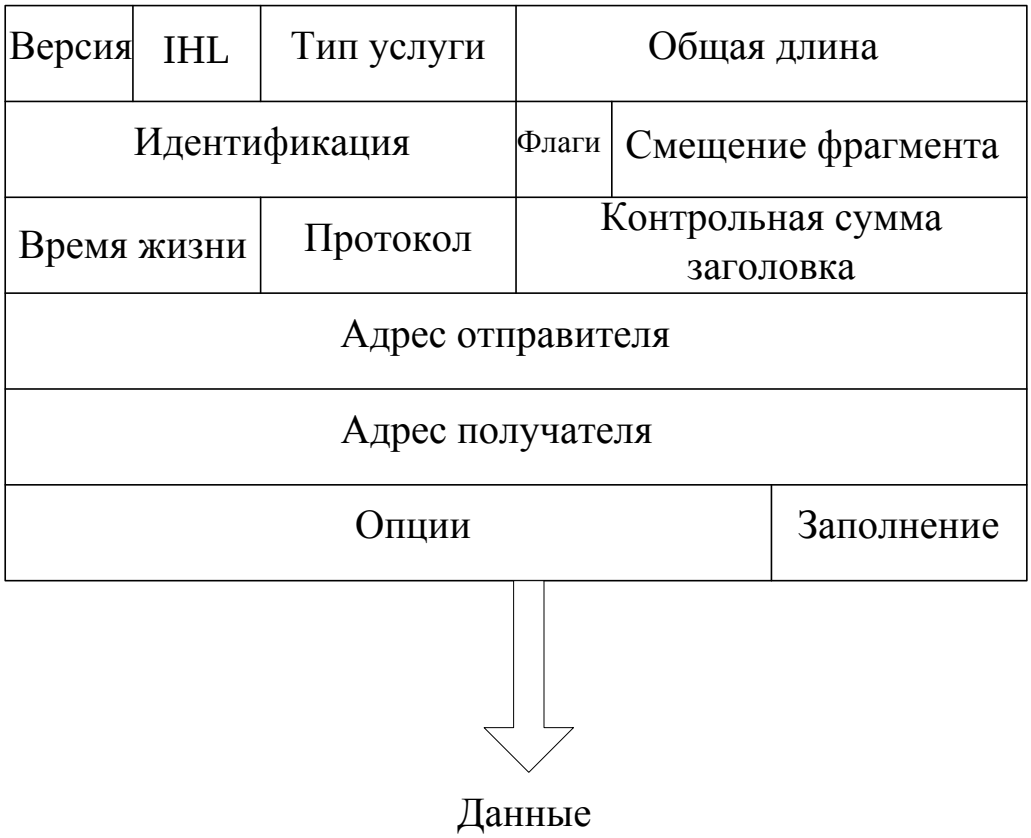
Протокол IPорганизует *пакетную передачу информации* от узла к узлу IPсети, не используя процедур установления соединения между источником и приемником информации. Кроме того, InternetProtocol является дейтаграммным протоколом: при передаче информации по протоколу IP, каждый пакет передается от узла к узлу и обрабатывается в узлах независимо от других пакетов.

Протокол IPне обеспечивает надежность доставки информации, так как он не имеет механизмов повторной передачи. Он не имеет также и механизмов управления потоком (flow-control). Дейтаграммы могут быть потеряны, размножены, или получены не в том порядке, в каком они были переданы.

Протокол IPбазируется на протоколе уровня звена данных,который обеспечивает передачу данных по физической среде. Программный модуль, реализующий протокол IP, определяет маршрут переноса данных по сети до точки назначения, или до промежуточного маршрутизатора, где дейтаграмма извлекается из кадра локальной сети и направляется в канал, соответствующему выбранному маршруту.Дейтаграммы могут разбиваться на более мелкие фрагменты, или наоборот, несколько дейтаграмм могут объединяться в одну на стыке разных сетей, еслиэти сети поддерживают передачу дейтаграмм разной длины.

В каждой рабочей станции, подключенной к IPсети, обработка IPдейтаграмм производится по одним и тем же *правилам адресации, фрагментации и маршрутизации.* Рабочие станции рассматривают каждую дейтаграмму как независимую протокольную единицу, так как протокол IPне использует логических соединений, или каких-либо других средств идентификации виртуальных каналов.

На нижеследующем рисунке показана структура протокольной единицы протокола – IP–дейтаграммы.



IP-дейтаграмма

*Поле «Версия (version)»*идентифицирует используемую версию протокола IP, в рассматриваемом случае указывается версия 4. Размерность поля 4 бита. Необходимость данного поля объясняется тем, что в переходный период в сети могут использоваться протоколы разных версий.

*Поле «Длина заголовка (headerlength)»*состоит из 4-х битов и определяет длину заголовка. Длина указывается по количеству блоков размером 32 бита каждый. В типичном случае значение этого поля равно 5.

*Поле «Тип обслуживания (TypeofService)»*содержит информацию, которая бывает нужна при поддержке сетью разных классов обслуживания. Использование этого поля в

Интернет будет возрастать по мере роста в IPсетях возможностей передачи мультимедийного трафика с задаваемыми параметрами качества обслуживания.

Поле «Общая длина (TotalLength)» состоит из двух байтов.Данное поле определяет общую длину дейтаграммы в октетах (в байтах), включая заголовок и полезную нагрузку. Максимальная длина дейтаграммы составляет 65535 октетов, однако, на практике, все рабочие станции и маршрутизаторы работают с длинами, не превышающими 576 байтов. Это объясняется тем, что при превышении указанной длины, снижается эффективность работы сети.

Протокол IPиспользует три поля заголовка для управления фрагментацией/сборкой дейтаграмм. Как уже упоминалось, фрагментация необходима потому что, разные сети, по которым передаются дейтаграммы, имеют разные максимальные размеры кадра.

«*Идентификатор фрагмента (identifier)»*обозначает все фрагменты одной дейтаграммы, что необходимо для ее успешной сборки на приемной стороне.

Поле «флаги (flags)» обеспечивает возможность фрагментации дейтаграммы, при использовании фрагментации, позволяет идентифицировать последний фрагмент дейтаграммы.

Поле «смещение фрагмента (FragmentOffset)» определяет положение фрагмента относительно исходной дейтаграммы в единицах равных 8 октетам.

*Поле «время жизни (TTL- TimeToLive)»*используется для ограничения времени, в течение которого дейтаграмма

находится в сети. Каждый маршрутизатор сети должен уменьшать значение этого поля на единицу, и отбрасывать дейтаграмму, если поле TTLприняло нулевое значение. Наличие поля TTLограничивает возможность бесконечной циркуляции дейтаграммы по сети, например, в случае, если по какой-либо причине маршрут, по которому она следует, оказался «закольцованным».

Поле «протокол (Protocol)» идентифицирует протокол верхнего уровня (TCP, UDPи т.д.).

*Поле «контрольная сумма заголовка (HeaderChecksum)»*обеспечивает возможность контроля ошибок в заголовке.

IP-дейтаграммы содержат в заголовке два адреса – отправителя (Source) и получателя (Destination), которые не меняютсяна протяжении всей жизни дейтаграммы.

БолееподробноструктураифункцииипротоколаIPv4 описанывRFC-791 (**InternetProtocol**DARPAINTERNETPROGRAMPROTOCOLSPECIFICATION).

В процессе эксплуатации IPпротокола выявился ряд проблем.

Проблемой IPпротокола стала нехватка адресного пространства, что в свою очередь, потребовало изменение формата адреса.

Другой проблемой является недостаточная масштабируемость процедуры маршрутизации – основы IPсетей. Быстрый рост сетей вызывает перегрузку маршрутизаторов, которые вынуждены поддерживать

таблицы маршрутизации с десятками и сотнями тысяч записей, а также решать проблемы фрагментации пакетов. Комитет IETFнамеревается решить существующие проблемы с помощью межсетевого протокола нового поколения – IPng, известного также, как IPv6.

Расширение адресного пространства

Протокол IPрешает потенциальную проблему нехватки адресов за счет расширения адреса до 128 бит, что было сделано с целью структурного изменения системы адресации и расширения ее функциональных возможностей.

Однако, такое существенное увеличение длины адреса было сделано, в значительной степени не с целью снять проблему дефицита адресов, а для повышения эффективности работы сетей на основе этого протокола. Вместо существующих *двух уровней иерархии адреса* в протоколе IPv6 предлагается использовать четыре уровня, что предполагает *трехуровневую идентификацию сетей* и *один уровень для идентификации узлов.* За счет увеличения числа уровней иерархии в структуре адреса, новый протокол эффективно поддерживает технологию агрегации адресов (CIDR), которая упоминалась выше. Благодаря этой особенности, а также усовершенствованной системе групповой адресации и введению нового типа адресов (anycast), IPv6 позволяет уменьшить затраты ресурсов оборудования на маршрутизацию.

В 6 версии протокола IPпринята новая форма записи адреса, так как при определении адреса сети, граница маски часто не совпадает с границей байтов адреса и десятичная запись в данном случае не удобна. Теперь адрес записывается в

шестнадцатеричном виде, причем каждые четыре цифры отделяются друг от друга двоеточием, например:

FEDC : 0A96 : 0 : 0 : 0 : 0 : 7733 : 567A

Для сетей, поддерживающих обе версии протокола – IPv4 и IPv6, имеется возможность использовать для младших 4 байтов традиционную десятичную запись, а для старших – шестнадцатеричную:

0: 0 : 0 : FFFP. 194. 135. 75. 104

Типы адресов

Для IPv6 определены следующие основные типы адресов:

- *unicast;*
- *multicast;*
- *anycast;*

Типы адресов определяются содержим*ым* нескольких старших битов адреса, которые получили название *префикса формата*.

Адрес типа *«unicast»* представляет собой *уникальный идентификатор сетевого интерфейса рабочей станции или маршрутизатора* и по смыслу полностью идентичен уникальному адресу IPv4. Однако, в версии 6 отсутствует понятие класса сети и фиксированное разбиение адреса на адрес сети и адрес узла по границам байтов.

Адрес типа *«multicast»* - *групповой адрес, необходимый для многоадресной рассылки*. Он характеризуется префиксом формата «11111111» и идентифицирует группу

интерфейсов, относящихся к разным рабочим станциям. Пакеты с такими адресами доставляются ко всем интерфейсам входящим в группу. Существует также предопределенный адрес, обозначающий все интерфейсы подсети. В составе *группового адреса IPv6* имеется поле *«scope» (область)*, которое определяет входят ли в группу рабочие станции одной подсети, всех подсетей предприятия или рабочие станции сети Интернет. Кроме того, предусмотрен признак постоянной или временной группы. Данное поле именуется *«Время жизни»* в формате группового*(Multicast)* адресаи может принимать одно из двух значений:*«0»*– «постоянно» и «*1»* – «временно».

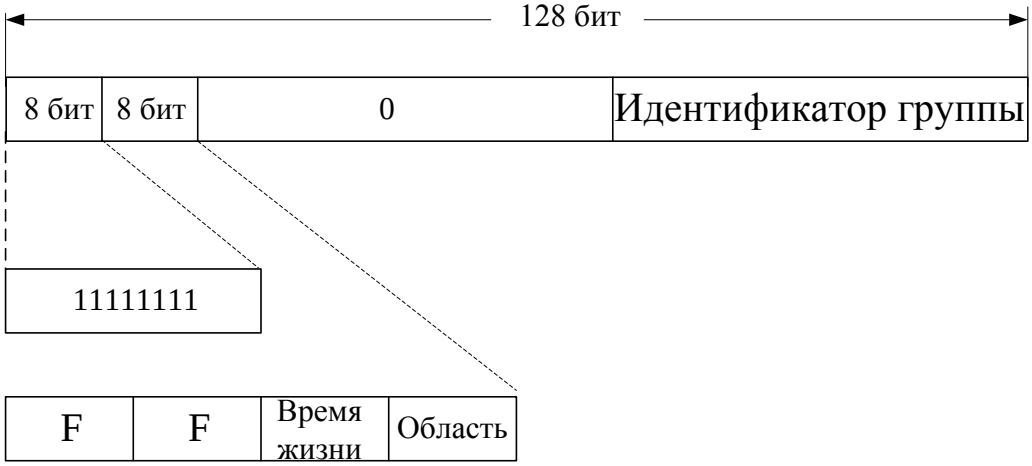
Адрес типа *«anycast»*является новым типом адреса, определяющий аналогично *«multicast»*группу интерфейсов, с тем отличием, что пакет, имеющий соответствующий тип адреса, доставляется не всем членам группы, а ближайшему «с точки зрения» маршрутизатора.Данный тип адреса синтаксически ничем не отличается от адреса типа *«unicast»*и выделяется из аналогичного диапазона.

«Anycast» адрес может быть присвоен только *сетевым интерфейсам маршрутизатора.* Интерфейсам маршрутизатора будут присваиваться *индивидуальные «unicast» адреса и общий «anycast» адрес.*Адреса *«anycast»*ориентированы на определение маршрута узлом – отправителем. Например, у абонента есть возможность обеспечить прохождение своих пакетов через сеть конкретного поставщика, указав в цепочке адресов маршрута «anycast» - адрес, присвоенный всем маршрутизаторам в сети этого поставщика. При этом пакет

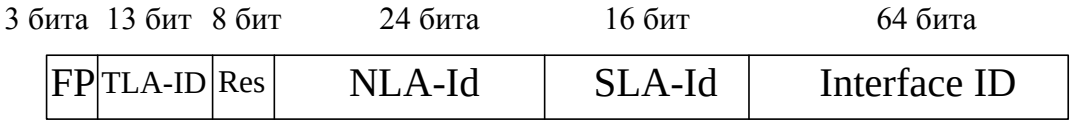
будет передан на «ближайший» подходящий маршрутизатор сети, первоначально установленный абонентом.

Форматы выборочного («Anycast») адреса, группового («Multicast») адреса, а также совместимость адресации IPv4 и IPv6 соответственнопредставлены на нижеследующих рисунках.

Групповой (Multicast) адрес



Выборочный (Anycast) адрес



Выборочный («Anycast») и групповой («Multicast») адреса

Полями выборочного (Anycast) адреса являются следующие (см. также рекомендации *RFC2373*):

- Форматныйпрефикс данного типа адресов, значение которого «001»;
- TLAId – идентификатор агрегации TLA-Idиспользуется маршрутизаторами крупнейших провайдеров и точек обмена трафиком для отправки их в определенную «подсеть»;
- Поле «Res» предназначено для увеличения других полей в случае возникновения в будущем такой необходимости;
- Идентификатор агрегации NLA Id предназначен для маршрутизаторов «подсетей»;
- Идентификатор SLAIdиспользуется для сетей отдельных организаций (корпоративных сетей, провайдеров и т.д.).

В групповом «Multicast» адресе поле «Время жизни» может принимать значения *«0»* - постоянно и *«1»* - временно.

Поле «Область» может принимать значения «1» - узел, «2»-канал, «5» - сеть абонента, «8» - организация, «E» - глобальный.

Совместимость адресации IPv4 и IPv6

	80 бит	16 бит	32 бита
Адреса IPv6 с вложенными адресами IPv4	0000……...0000	0000	Адрес IPv4

	80 бит	16 бит	32 бита
Адреса IPv6 с отображаемыми адресами IPv4	0000……...0000	FFFF	Адрес IPv4

Совместимость адресации IPv4 и IPv6

Например,IPадрес имеет вид «0:0:0:0:0:0:192.168.30.1». Тогда,X= «0000»соответствует совместимым, аX= «FFFF» отображаемым IP адресам.

Например,::192.168.30.1 (совместимый), а ::FFFF:192.168.30.1 (отображаемый).

В рамках системы адресации IPv6 имеется также выделенное пространство адресов для локального использования, т.е. для сетей, не входящих в Интернет. Существует две разновидности локальных адресов:

- Для *«плоских»* сетей не разделенных на подсети (Link-Local);
- Для сетей, разделенных на подсети *(«Site-Local»).* На нижеследующем рисунке представлены форматы параметров локальной адресации интерфейсов локальной сети.

Link-local (используются при автоконфигурации и при отсутствии маршрутизаторов)

10 бит		64 бита
1111111010	0……0	Идентификатор интерфейса

Link-local (эквивалентны частным адресам в IPv4)

10 бит		16 бит	64 бита
1111111011	0…...0	SLA	Идентификатор интерфейса
		Идентификатор подсети	

Форматы параметров локальной адресации

Для локальной адресации используются префиксы:

1111111010 – Link-local;

1111111011 – Site-local;

11111111 – Multicast.

Изменение формата заголовков пакетов

Система адресации IPv6 использует свой собственный формат заголовка. В данном формате используется новая схема организации «вложенных заголовков», обеспечивающие разделение заголовка на*основной* и *дополнительные.*

Основной заголовок содержит необходимый минимум обязательной информации, в то время как дополнительный заголовок включает в себя необязательные параметры, которые могут отсутствовать. Основной заголовок дейтаграммы IPv6 длиной 40 байтов имеет формат, представленный на следующем рисунке:

<table>
<tr><td>Версия
(4 бита)</td><td>Класс трафика
(8 битов)</td><td colspan="3">Метка потока (20 битов)</td></tr>
<tr><td colspan="2">Длина (16 битов)</td><td colspan="2">След. Заголовок
(8 битов)</td><td></td></tr>
<tr><td colspan="5">Адрес отправителя (128 битов)</td></tr>
<tr><td colspan="5">Адрес получателя (128 битов)</td></tr>
</table>

Формат основного заголовка дейтаграммы IPv6

- Поле *«Класс трафика»*(***«TrafficClass»)***эквивалентно по назначению полю *«Тип обслуживания»****(«Type of service»);***
- Поле *«Лимит переходов» («HopLimits»)* эквивалентно по назначению полю «Вре*мя жизни» («TimeToLiv*е) протокола IPv4, кратко рассмотренного ранее. Поле *«Метка потока» («FlowLabel»)*позволяет выделить и обрабатывать отдельные потоки данных не загружая маршрутизаторы для обработки *параметров маршрутизации.*Например, по одному потоку (маршруту) могут передаваться пакеты разных приложений*;*
- Поле*«Следующий заголовок»* является аналогом поля *«Протокол» («Protocol») IPv4* и определяет тип заголовка, следующего за основным. Каждый следующий дополнительный заголовок также содержит поле «NextHeader». В случае отсутствия дополнительных заголовков, то это поле содержит содержит значение, присвоенное тому из протоколов TCP, UDP, OSPF, который используется для переноса полезной нагрузки данной дейтаграммы*;*

В рамках спецификаций IPv6 определены заголовки следующих типов:

- Заголовок *«Routing»* содержит информацию о маршруте, выбранном отправителем дейтаграммы;

- Заголовок *«Fragmentation»*содержит информацию о фрагментации дейтаграмм*ы* и обрабатывается только конечными узлами сети.
- Заголовок *«Authentication»*содержит информацию, необходимую для проверки полномочий на доступ к сети отправителя дейтаграммы.
- Заголовок *«Encapsulation»*содержит информацию, необходимую для обеспечения конфиденциальности данных путем шифрования.
- Заголовок*«Hop-by-HopOptions»* - специальные параметры обработки пакетов на участках их приемопередачи.
- Заголовок *«DestinationOptions»*дополнительные параметры для узла назначения.