МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__»_____2017 г.

Структура сообщений сетевого уровня в IP-сети

Методические указания по выполнению практической работы по дисциплине «Введение в специальность» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621(076.1)
Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Структура сообщений сетевого уровня в IP-сети: методические указания по выполнению практической работы по дисциплине «Введение в специальность» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 16 с.: ил., Библиогр.: с. 16.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать. 15.12.17. Формат 60x84 1/16.
Усл. печ. л.0,9.Уч. –изд.л. 0,8. Тираж 30 экз. Заказ2953.Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября

Содержание

1. Цель практической работы:

Ознакомление с принципами и методами адресации и передачи на сетевом уровне сообщений в IP-сети передачи данных на примере структуры дейтаграммы.

2. Краткие теоретические сведения

Адресация в IP-сетях

Каждый терминал в сети TCP/IP имеет адреса трех уровней.

1. *Физический (MAC-адрес)* - локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, куда входит данный узел.
2. *Сетевой (IP-адрес)*, состоящий из 4 байтов, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно или назначен по рекомендации специального подразделения Интернета (Network Information Center, NIC), если сеть должна работать как составная часть Интернета. Обычно провайдеры услуг Интернета получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

   Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма условно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.
3. *Символьный (DNS-имя)* - идентификатор-имя. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена.

Интернет - это совокупность тысяч компьютеров, объединенных в сети, которые, в свою очередь, соединены между собой посредством маршрутизаторов.

Сеть Интернет имеет иерархическую структуру. Этот подход является эффективным, потому что позволяет идентифицировать компоненты Интернета посредством адресов, также имеющих иерархическую структуру. Старшие

биты адреса идентифицируют сеть, в которой находится рабочая станция, а младшие - расположение рабочей станции в этой сети.

Подавляющее большинство сетей сейчас использует протокол *IPv4 (интернет-протокол версии 4)*, хотя уже разработана шестая версия протокола IP. Схема адресации протокола IPv4 предусматривает размер адресного поля 32 бита, что дает 2^{32} (или 4 294 967 296) потенциальных адресов.

IP-адрес 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, D или E). Область сетевого идентификатора (Network ID) определяет конкретную сеть в классе, а область Host ID идентифицирует конкретный компьютер в сети, а именно:

- адреса класса A идентифицируются начальным битом 0. Следующие семь битов определяют конкретную сеть (число возможных значений - 128, или 2^7). Остальные 24 бита определяют конкретный компьютер в сети, при возможном количестве компьютеров 16 777 216 (2^{24}). Адреса класса A предназначены для очень крупных сетей с большим количеством рабочих станций;
- адреса класса B идентифицируются начальной двухбитовой двоичной последовательностью 10. Следующие 14 битов определяют сеть, при возможном количестве сетей 16 384 (2^{14}). Остальные 16 битов определяют конкретный компьютер, с возможным количеством компьютеров 65 536 (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, и оставшиеся 28 битов определяют групповой адрес;
- адреса класса E идентифицируются начальной четырехбитовой двоичной последовательностью 1111. Адреса этого класса зарезервированы для будущего использования.

Рисунок 1 - Структура IP-адреса

Способ, при помощи которого записываются все IP-адреса, 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 0-255). Адреса класса A начинаются с 1 до 127, адреса класса B - с 128 до 191, и адреса класса C - с 192 до 223.

Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Строго говоря, адрес идентифицирует только сетевой интерфейс рабочей станции, т. е. точку подключения к сети.

IP-адреса распределяются *Корпорацией Интернет по присвоению имен и номеров (ICANN)*. Класс IP-адреса 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 IP-адреса к конкретному компьютеру. При *динамической адресации* компьютеру присваивается доступный IP-адрес всякий раз при установлении соединения. Динамическое присвоение IP-адресов 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.

Как уже отмечалось, протокол IP версии 4 предусматривает размер адресного поля 32 бита, что дает 2^{32} (или 4 294 967 296) потенциальных адресов. Однако возрастающая популярность технологии TCP/IP привела к истощению плана нумерации протокола. Дополнительной проблемой является тот факт, что очень большое количество адресов класса A и класса B было выделено крупным организациям, которые в них на самом деле не нуждались, и поскольку фактически использовался только небольшой процент адресов, огромное количество доступных адресов было потеряно.

Протокол IPv6 решает этот вопрос путем расширения адресного поля до 128 битов, обеспечивая тем самым 2^{128} потенциальных адресов, что составляет величину 340.282.366.920.938.463.463.374.607.431.768.211.456.

Протокол IPv6 обладает также дополнительными функциональными возможностями, хотя для их реализации потребуется модернизация существующего сетевого программного обеспечения.

Но вернемся к протоколу IPv4. Компьютер, подключенный к сети Интернет, кроме IP-адреса может идентифицироваться доменным именем. Сеть Интернет разделена на логические области (домены). Адреса в *системе имен доменов (DNS)*, администрирование которых лежит на ICANN, имеют стандартный вид: последовательность имен, разделенных точками. Домены TLD, которые идентифицируются как суффикс доменного имени, бывают двух типов: *обобщенные домены верхнего уровня* (net, com, org) и *коды стран* (ru, fi, ua).

Имена доменов гораздо легче запомнить и ввести, но необходимо преобразование для перевода имен доменов в IP-адреса - для того, чтобы разные маршрутизаторы и коммутаторы могли направить информацию в нужный пункт назначения.

Модель OSI

Функционирование сети Интернет основано на сложном комплексе протоколов, обеспечивающих выполнение различных функций - от непосредственно передачи данных до управления конфигурацией оборудования сети.

Для того, чтобы классифицировать различные протоколы и понять их место в общей структуре технологии межсетевого взаимодействия, удобно воспользоваться так называемым "многоуровневым представлением сетевых протоколов". В рамках такого представления подразумевается, что протоколы более высокого уровня используют функции протоколов более низкого уровня. Классической моделью такого рода является семиуровневая модель взаимодействия открытых систем (Open Systems Interconnection - OSI), разработанная ITU-T.

Первый уровень модели - уровень сетевого интерфейса - поддерживает физический процесс переноса информации между устройствами в сети, т. е. объединяет функции двух уровней OSI - физического и звена данных. Второй уровень сетевого интерфейса обеспечивает физическое соединение со средой передачи, обеспечивает разрешение конфликтов, возникающих в процессе организации доступа к среде (например, используя технологию CSMA/CD в сети Ethernet), упаковывает данные в пакеты. Пакет - это протокольная единица, которая содержит информацию верхних уровней и служебные поля (аппаратные адреса, порядковые номера, подтверждения и т. д.), необходимые для функционирования протоколов этого уровня.

Рисунок 2 - Уровни модели OSI

Сетевой уровень отвечает за передачу информации, упакованной в дейтаграммы (datagram), от одного компьютера к другому. Дейтаграмма - это протокольная единица, которой оперируют протоколы семейства TCP/IP. Она содержит адресную информацию, необходимую для переноса дейтаграммы через сеть, а не только в рамках одного звена данных. Понятие дейтаграммы никак не связано с физическими характеристиками сетей и каналов связи, что подчеркивает независимость протоколов TCP/IP от аппаратуры. Основным протоколом, реализующим функции сетевого уровня, является протокол IP. Этот протокол отвечает за маршрутизацию, фрагментацию и сборку дейтаграмм в рабочей станции.

Обмен между сетевыми узлами информацией о состоянии сети, необходимой для формирования оптимальных маршрутов следования дейтаграмм, обеспечивают протоколы маршрутизации - RIP, EGP, BGP, OSPF и др.

Протокол преобразования адресов (Address Resolution Protocol - ARP) преобразует IP-адреса в адреса, использующиеся в локальных сетях (например, Ethernet). На некоторых рисунках, изображающих архитектуру и взаимосвязь протоколов, ARP размещают ниже IP, чтобы показать его тесную взаимосвязь с уровнем сетевого интерфейса.

Протокол контрольных сообщений - (Internet Control Message Protocol - ICMP) предоставляет возможность программному обеспечению рабочей станции или маршрутизатора обмениваться информацией о проблемах маршрутизации пакетов с другими устройствами в сети. Протокол ICMP - необходимая часть реализации стека протоколов TCP/IP.

Когда дейтаграмма проходит по сети, она может быть потеряна или искажена. Транспортный уровень решает эту проблему и обеспечивает надежную передачу информации от источника к приемнику. Кроме того, реализации протоколов этого уровня образуют универсальный интерфейс для приложений, дающий доступ к услугам сетевого уровня. Наиболее важными протоколами транспортного уровня являются TCP и UDP.

Конечные пользователи взаимодействуют с компьютером на уровне пользовательских приложений. Разработано множество протоколов, применяемых соответствующими приложениями. Например, приложения передачи файлов используют протокол FTP, веб-приложения - протокол HTTP. Оба протокола, FTP и HTTP, базируются на протоколе TCP. Приложение Telnet обеспечивает подключение удаленных терминалов. Протокол эксплуатационного управления сетью SNMP позволяет управлять конфигурацией оборудования в сети и собирать информацию о его функционировании, в том числе и об аварийных ситуациях. Приложения, созданные для организации речевой связи и видеосвязи, используют протокол RTP для передачи информации, чувствительной к задержкам. X Window - популярный протокол для подключения к интеллектуальному графическому терминалу. Этот список можно еще продолжить рядом протоколов.

Таким образом, IP-сети используют для передачи информации разнообразные протоколы, причем функции протоколов не зависят от того, какие данные передаются. Иными словами, IP, ARP, ICMP, TCP, UDP и другие элементы стека протоколов TCP/IP предоставляют универсальные средства передачи информации, какой бы природы она ни была (файл по FTP, веб-страница или аудиоданные).

Основные протоколы IP-телефонии

Протокол IP версии 4

В качестве основного протокола сетевого уровня в стеке протоколов TCP/IP применяется протокол IP, который изначально проектировался как протокол передачи пакетов в сетях, состоящих из большого количества локальных сетей. Поэтому он хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP организует пакетную передачу информации от узла к узлу IP-сети, не используя процедур установления соединения между источником и приемником информации. Кроме того, Internet Protocol 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 IP не обеспечивает надежность доставки информации, так как он не имеет механизмов повторной передачи. Он не имеет также и механизмов управления потоком данных (flow-control). Дейтаграммы могут быть потеряны, размножены или получены не в том порядке, в каком были переданы.

Протокол IP базируется 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, который соответствует выбранному маршруту. Дейтаграммы могут разбиваться на более мелкие фрагменты, или, наоборот, несколько дейтаграмм могут объединяться в одну на стыке разных сетей, если эти сети поддерживают передачу дейтаграмм разной длины.

В каждой рабочей станции, подключенной к IP-сети, обработка IP-дейтаграмм производится по одним и тем же правилам адресации, фрагментации и маршрутизации. Рабочие станции рассматривают каждую дейтаграмму как независимую протокольную единицу.

На рисунке 3 показана структура протокольной единицы протокола IP-дейтаграммы.

Поле версия (version) идентифицирует используемую версию протокола IP, в рассматриваемом случае указывается версия 4. Необходимость этого поля объясняется тем, что в переходный период в сети могут применяться протоколы разных версий.

Поле длина заголовка (header length), состоящее из 4 битов, определяет длину заголовка, причем длина указывается как количество блоков размером 32 бита. В типичном случае значение этого поля равно 5.

Версия (Version)		*Длина заголовка*
Тип обслуживания		
Общая длина		
Идентификатор фрагмента		
Флаги		Смещение фрагмента
Время жизни		
Протокол		
Контрольная сумма заголовка		
Адрес отправителя		
Адрес получателя		
Опциональные поля и заполнение		
Данные		

Рисунок 3 - IP-дейтаграмма

Поле Тип обслуживания (Type of Service) содержит информацию, которая бывает нужна при поддержке сетью разных классов обслуживания. Использование этого поля в Интернете будет возрастать по мере роста в IP-сетях возможностей передачи мультимедийного трафика с задаваемыми параметрами качества обслуживания.

Поле Общая длина (Total Length) определяет общую длину дейтаграммы в октетах (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 IP использует 3 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 Флагов (Flags) обеспечивает возможность фрагментации дейтаграмм и, при использовании фрагментации, позволяет идентифицировать последний фрагмент дейтаграммы.

Поле Смещение фрагмента (Fragment Offset) определяет положение фрагмента относительно исходной дейтаграммы в единицах, равных 8 октетам.

Поле Время жизни (TTL - Time To Live) 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 TTL приняло нулевое значение. Наличие поля TTL ограничивает возможность бесконечной циркуляции дейтаграммы по сети.

Поле Протокол (Protocol) идентифицирует протокол верхнего уровня (TCP, UDP и т. д.).

Поле Контрольная сумма заголовка (Header Checksum) обеспечивает возможность контроля ошибок в заголовке. Алгоритм подсчета контрольной суммы весьма прост, поскольку обычно протоколы нижнего уровня имеют более развитые средства контроля ошибок.

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

3. Практическое задание

1. При подготовке к практическому занятию изучить следующие вопросы:

- IP-протоколы передачи данных сетевого уровня;
- назначение IP-протоколов;
- структуры дейтаграмм, назначение полей дейтаграммы;
- методы адресации в IP-сетях;
- классы IP-сетей и структура адреса в IP-сети.

2. Получить вариант задания у преподавателя и в соответствии с заданным вариантом таблицы 8.1 идентифицировать класс сети, определить количество хостов, выбрать маску подсети и создать таблицу маршрутизации.

Дана сеть, состоящая из B подсетей и IP-адресами A.A.x.x. Требуется идентифицировать класс сети, определить количество хостов, выбрать маску подсети и привести структуру IPv4-дейтаграммы, содержащей кодированное кодом Windows-1251 произвольное текстовое сообщение (не более 5 символов), передаваемое от хоста 1 подсети 1 к хосту 2 подсети B.

При этом структура дейтаграммы согласно рис. 8.1 должна включать несущественные поля в общем виде, а в полях IP-адреса отправителя, и IP-адреса получателя в качестве их содержимого должны быть приведены в двоичной форме адреса любых хостов из, соответственно, сети 1 и сети 2 – согласно выбранному варианту. В поле данных должно быть приведено в коде Windows-1251 любое русское слово из 4-х букв, например, «небо» (должно быть разное в каждом варианте).

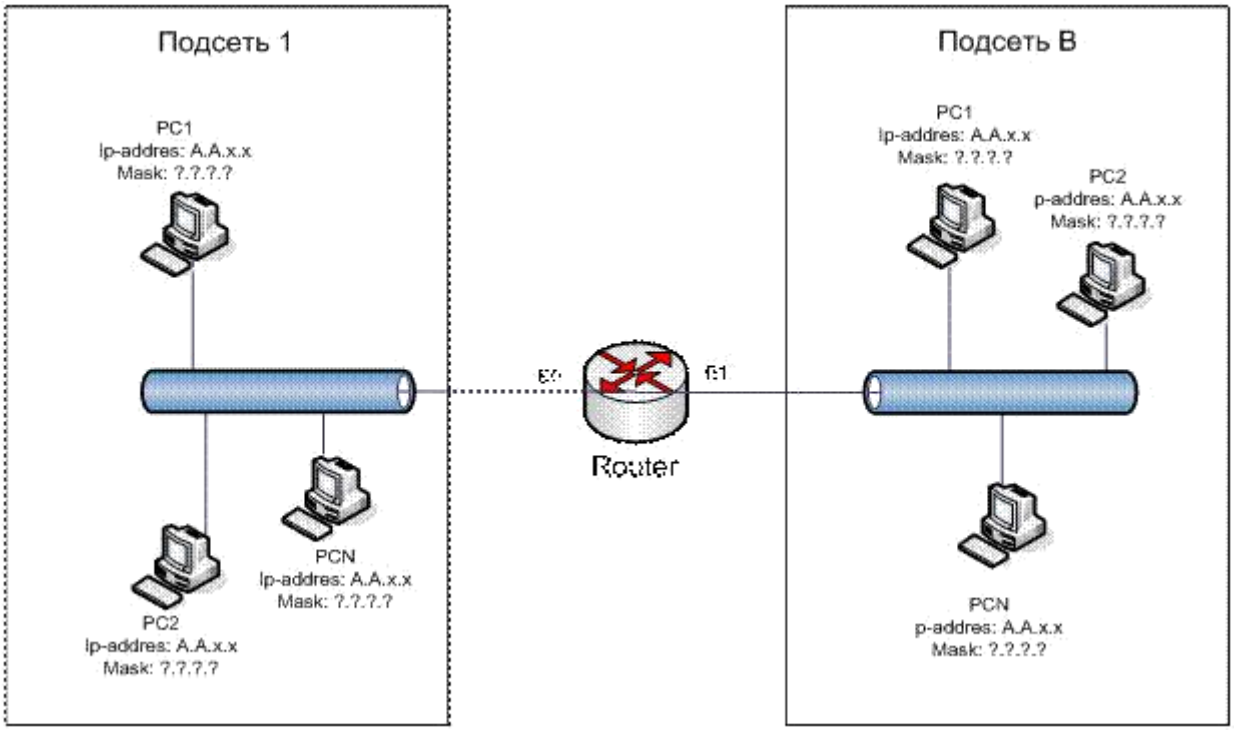

Рисунок 4 - Схема организации сети (значение A и B даны согласно варианту)

Таблица.1. Варианты заданий.

Вариант	IP-address (A)	Количество подсетей (B)
1	172.16.x.x	254
2	192.168. x.x	62
3	213.206. x.x	14
4	176.32.x.x	6
5	196.120. x.x	30
6	206.168.x.x	2
7	170.144.. x.x	126
8	177.168. x.x	14
9	186.124. x.x	62
10	188.24. x.x	2
11	198.168. x.x	6
12	127.254. x.x	254
13	197.34. x.x	62
14	172.16. x.x	30
15	192.168. x.x	14

4. Порядок выполнения задания

При выполнении задания рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данному практическому занятию.
2. Получить у преподавателя задание.
3. Выполнить практическую часть.
4. Ответить на контрольные вопросы.

5. Содержание отчета

1. Краткие теоретические сведения по структуре дейтаграмм и методам их адресации в заданной сети.

2. Выполненное задание, по заданному варианту.

6. Контрольные вопросы

1. На каком уровне ЭМВОС используются IP-протоколы.

2. Назначение IP-протокола.

3. Что понимается под ***маршрутизацией*** IP-пакетов.

4. Что такое IP-дейтаграмма, приведите ее структуру для IPv4.

5. Дайте определение IP-адреса.

6. Перечислите виды IP-адресов.

7. Что такое маска сети и маска подсети и как они определяются.

8. Как с помощью масок сети или подсети выделить из сетевого адреса адрес конкретной сети и хоста в ней.

9. Сущность кодирования текста кодом Windows-1251.

Библиографический список

1. Куроуз Дж., Росс К. Компьютерные сети. 2-е изд. – СПб.: Питер, 2004. -765 с.
2. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
3. Материалы курса «IP-телефония» сайта Интранет ТУИТ http://www.teic.uz/dlnet.
4. Стандарт RFC-791.