МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационных систем и технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
« 16 » 04 2019 г.

Сетевые технологии

Методические указания по выполнению лабораторных работ для направления подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем»

Курск 2019

УДК 004

Составитель А.С. Сизов

Рецензент
Кандидат технических наук, доцент Ю.А. Халин

Сетевые технологии: методические указания по выполнению лабораторных работ для направления подготовки «Математическое обеспечение и администрирование информационных систем» / Юго-Зап. гос. ун-т; сост. А.С. Сизов. Курск, 2019. 41 с.: Библиогр.: с. 41.

Методические рекомендации предназначены для студентов, обучающихся по направлению подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем»

Текст печатается в авторской редакции.

Подписано в печать 16.04.19 . Формат 60x84 1/16.
Усл.печ. л. 2,4 . Уч.-изд. л. 2,2 . Тираж 100 экз.
Заказ. 335 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

Содержание

Введение

Основой конкретной сетевой технологии является протокол, либо семейство протоколов, представленное стандартными спецификациями. Затем протокол реализуется в виде программного обеспечения, либо специализированного сетевого устройства, такого как сетевой адаптер, модем, коммутатор, маршрутизатор, конвертор интерфейсов, из которых строятся сети. Именно поэтому основное внимание уделяется изучению стандартных спецификаций протоколов и вопросам взаимодействия протоколов различных уровней в процессе инкапсуляции информации, а также вопросам доставки информации (пакетов) по назначению.

Основой для углублённого изучения протоколов и их взаимодействия является анализ трафика с полной интерпретацией передаваемых потоков битов (байтов), выделением заголовков пакетов и их полей, установлению взаимосвязей между заголовками различных уровней. Для этих целей использован программный анализатор трафика Ethereal, позволяющий записать передаваемые в сети пакеты и выполнить их автоматизированную интерпретацию. На практических занятиях решаются также задачи построения заголовков пакетов в процессе их инкапсуляции. Таким образом, имитируется работа как передающей, так и принимающей подсистем.

Изучено доминирующее на рынке семейство протоколов сетевого-сеансового уровней TCP/IP и их инкапсуляция в такие протоколы канального уровня как IEEE 802.3* (Ethernet) и PPP. Выбор канальных технологий обусловлен их широким применением в магистралях DWDM.

Вопросы доставки пакетов (кадров) в сетях составляют вторую часть материала настоящих указаний. Изучение организовано по нарастанию сложности технологий: коммутация кадров Ethernet, статическая маршрутизация в IP-сетях, протоколы динамической маршрутизации RIP, OSPF, BGP и, наконец, современная технология коммутации меток MPLS, интегрирующая принципы коммутации пакетов и коммутации каналов. Для изучения вопросов маршрутизации в сетях использована моделирующая система Opnet, позволяющая имитировать процессы создания таблиц маршрутизации (коммутации) для заданной структурной схемы сети.

Лабораторная работа №1
Передача IP-трафика в сетях Ethernet

Цель работы: изучить особенности инкапсуляции IP-пакетов в Ethernet-фреймы и отображения IP-адресов на MAC-адреса Ethernet

Подготовка:

- знать структуру заголовка Ethernet-фрейма
- знать структуру заголовка IP-пакета
- знать структуру запросов/ответов протокола ARP
- знать команды работы с ftp-сервером, команды отображения таблиц ARP/RARP

Задание: выполнить трассировку процессов формирования ARP-таблиц и передачи IP-
трафика в Ethernet с помощью анализатора трафика

Порядок выполнения работы

1. Запустить анализатор трафика и установить фильтр для отображения ARP-пакетов
2. Включая/выключая другие хосты сети и проверяя их доступность с помощью команды ping выполнить трассировку процессов заполнения APR-таблиц. Отобразить на экране построенные таблицы.
3. Установить фильтр для отображения ftp-трафика.
4. Выполнить трассировку передачи известного файла с ftp-сервера.

Варианты задания: IP, MAC-адреса компьютера, на котором выполняется работа.

Дополнительные требования:

1. Отобразить процесс формирования ARP-таблиц не менее чем для четырёх хостов.
2. Отобразить процесс получения не менее чем четырёх IP-пакетов.
3. Отобразить поля заголовков, задающих взаимодействие протоколов канального - сетевого, сетевого – транспортного уровней при инкапсуляции.
4. Один из фреймов представить в исходной (шестнадцатеричной) форме с интерпретацией всех полей IP и Ethernet-заголовков.

Содержание отчёта:

- структуры заголовков Ethernet-фрейма и IP-пакета
- структура запросов/ответов протокола ARP
- трасса процесса построения ARP таблиц (последовательность запросов/ответов)
- построенные ARP, RARP-таблицы
- трасса процессов передачи IP-пакетов
- полная интерпретация одного из фреймов по шестнадцатеричному представлению

Указания по выполнению работы:

Использовать анализатор пакетов Ethereal либо tcpdump (windump). Выбрать интерфейс (карта Ethernet). Установить требуемый фильтр (arp, ftp) и запустить запись передаваемых фреймов. Остановит процесс записи фреймов.

Использовать сохранённые фреймы для написания отчёта.

Команды ARP:

-a: отображает текущие ARP-записи, опрашивая текущие данные протокола
-g: то же что и -a

inet_addr: определяет IP-адрес

-N if_addr: отображает ARP записи для заданного в if_addr сетевого интерфейса
-d: удаляет узел
-s: добавляет узлы и связывает internet адреса с физическими адресами

Задание: Представить не менее 4 пакетов и 1 в hex виде.

Вход в систему:
login: student**04**

password: student

startx &

В одном окне xterm запускаем команду:

sudo ethereal

Трафик создается: в другом окне xterm запускаем команду ftp (жирным шрифтом отмечен ввод пользователя. Имя, пароль, и ip-адрес сервера приведены для примера и могут отличаться).

ftp 192.168.0.145

Name (192.168.0.145): **dmitry**

Password: **daze**

230 User dmitry logged in. Remote
system type is UNIX.
Using binary mode to transfer files. ftp>_

После успешной аутентификации на сервере, можно использовать следующие команды:

ftp>**dir** (Просмотр текущего каталога ftp) ftp>**get** ***имя_файла*** (Скачать файл с сервера) ftp>**quit** (Выход из ftp)

Команда оболочки cat выводит содержимое файла указанного в качестве первого аргумента

cat rfc903.txt

Перед выполнением команды get включаем прослушку Capture → Interface → Capture После получения файла нажимаем Stop (остановить прослушку и просмотреть результаты)

В hex (16-ричном) виде:

0000 00 80 48 67 8d 73 00 16 76 82 3b 3a 00 00 45
0010 00 84 9b 1f 00 00 40 11 37 2b e0 a8 00 0f c0
0020 00 91 03 fc 08 01 00 70 ea 05 00 00 3b 3a 08
0030 00 00 00 00 00 02 00 01 76 82 3b 33 c0 a8
0040 00 04 00 00 00 01 00 00 33 e2 c0 00 00 14

В текстовом:

1)

0.000000 192.168.0.207 192.168.0.145 TCP 62276>ftp

[syn] seq=0 mss=1460 ws=1 tsv=2395351 tser=0 Frame 1 (78
bytes on wire, 78 bytes captured)

Ethernet II, src: Intel_82:3b:3a(00:16:76:82:3b:3a) dst:
Compex_b7:bd:73(00:80:48:b7:bd:73)

Internet Protocol, Src: 192.168.0.207(192.168.0.207), Dst: 192.168.0.145
(192.168.0.145)

Transmission Control Protocol, Src Port: 62276 (62276), Dst Port: ftp (21), Seq: 0, Ack: 0, Len:

0

2)

0.000129 192.168.0.145 192.168.0.207 TCP ftp>62276

[syn, ack] Seq=0 Ack=8 Win=1448 Len=0 TSV=125099355 TSER=72740216

Frame2 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: Compex_b7:bd:73(00:80:48:b7:bd:73), Dst: Intel_82:3b:3a(00:16:76:82:3b:3a) Internet Protocol, Src: 192.168.0.145 (192.168.0.145), Dst: 192.168.0.207(192.168.0.207)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 62276 (62276), Seq: 0, Ack: 8, Len:

0

3)

Frame 21 (83 bytes on wire, 83 bytes captured)

Arrival Time: Feb 17, 2007 15:19:50.726006000

[Time delta from previous packet: 0.005147000 seconds] [Time since reference or first
frame: 7.438924000 seconds] Frame Number: 21

Packet Length: 83 bytes Capture
Length: 83 bytes [Frame is marked:
False]

[Protocols in frame: eth:ip:tcp:ftp] [Coloring Rule
Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: Intel_82:3b:3a(00:16:76:82:3b:3a), Dst: Compex_b7:bd:73(00:80:48:b7:bd:73) Destination: Compex_b7:bd:73(00:80:48:b7:bd:73)

Address: Compex_b7:bd:73(00:80:48:b7:bd:73)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default) Source: Intel_82:3b:3a(00:16:76:82:3b:3a)

Address: Intel_82:3b:3a(00:16:76:82:3b:3a)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default) Type: IP (0x0800)

Internet Protocol, Src: 192.168.0.207(192.168.0.207), Dst: 192.168.0.145 (192.168.0.145)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00) 0001 00.. = Differentiated Services Codepoint: Unknown (0x04)

.... ..0. = ECN-Capable Transport (ECT): 0

....0 = ECN-CE: 0

Total Length: 69

Identification: 0x6484 (25729) Flags: 0x04
(Don't Fragment) Fragment offset: 0

Time to live: 64 Protocol:
TCP (0x06)

Header checksum: 0x5371 [correct] Source:
192.168.0.207(192.168.0.207)

Destination: 192.168.0.145 (192.168.0.145)

4)

Frame 22 (76 bytes on wire, 76 bytes captured) Internet Protocol

Version: 4

Header length: 20 bytes Total
Length: 60

Flags: 0x04 (Don't Fragment) Fragment
offset: 0

Time to live: 64 Protocol:
TCP (0x06)

Header checksum: 0x3e47 [correct]

ARP:

1. arp -a
   192.168.0.145 at 00:80:48:b7:bd:73 on r10 [ethernet] 192.168.0.205 at 00:16:76:82:3b:a6 on r10 permanent [ethernet]

2. ping 192.168.0.102

   PING 192.168.0.102 (192.168.0.102) 56(84) bytes of data.

   64 bytes from 192.168.0.102: icmp_seq=1 ttl=63 time=6.45ms

   64 bytes from 192.168.0.102: icmp_seq=2 ttl=63 time=2.63ms

   64 bytes from 192.168.0.102: icmp_seq=3 ttl=63 time=2.05ms

   64 bytes from 192.168.0.102: icmp_seq=4 ttl=63 time=1.93ms

   --- 192.168.0.102 ping statistics ---

   4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev = 1.937/3.269/6.459/1.861 ms

Выполнение лабораторного задания:

В данной лабораторной работе будем использовать следующие команды.

- arp- a - просмотр имеющихся в таблице IP-адресов.
- ipconfig – определение собственного ip-адреса
- ping – пеленгование («присоединение») чужого ip-адреса.

ARP-запрос/ответ – выглядит следующим образом:

0.000000 Intel _82:3b:85 broadcast

ARP who has 192.168.0.208 Tell 192.168.0.203.

Рассмотрим два фрейма:

1) **Frame 1** (*60 bytes*)

Ethernet II: Src:Intel_82:3b:85 (00:16:7b:82:3b:85), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (**REQUEST**)

Type:ARP (0x0806);

Hardware size: 6;

Protocol size: 4;

Opcode: request (0x0001);

Sender MAC-address: Intel_82:3b:85 (00:16:76:82:3b:85);

Sender IP-address: 192.168.0.203 (192.168.0.203);

Target MAC-address: 00:00:00:00:00:00;

Target IP-address: 192.168.0.208 (192.168.0.208);

	Dst	*Src*	*Type ARP*	*Ethernet (0x0001)*
0000	ffffffffffff	001676823b85	0806	0001

IP (0x0800) *size (6)* *size (4)* *opcode* *sender MAC-address* *sender IP-address*

0010 0800 06 04 0001 001676823b85 c0a800cb

target MAC-address target IP-address
0020 000000000000 c0a800d0

2) Frame 2 (*60 bytes*)

Ethernet II: Src: Intel_82:3b:85 (00:16:76:82:3b:85), Dst: Intel_82:3b:b4 (00:16:76:82:3b:b4);

Address Resolution Protocol (**REPLY**)

Type:ARP (0x0806);

Hardware size: 6;

Protocol size: 4;

Opcode: reply (0x0002);

Sender MAC-address: Intel_82:3b:b4 (00:16:76:82:3b:b4);

Sender IP-address: 192.168.0.208 (192.168.0.208);

Target MAC-address: Intel_82:3b:85 (00:16:76:82:3b:85);

Target IP-address: 192.168.0.203 (192.168.0.203);

Dst *Src* *Type ARP* *Ethernet (0x0001)*
0000 001676823b85 001676823bb4 0806 0001

IP (0x0800) *size (6)* *size (4)* *opcode* *sender MAC-address* *sender IP-address*
0010 0800 06 04 0002 001676823bb4 c0a800d0

target MAC-address target IP-address
0020 001676823b85 c0a800cb

Контрольные вопросы:

1. Перечислить основные поля заголовка Ethernet.
2. Перечислить основные поля заголовка IP.
3. Перечислить основные поля ARP запроса/ответа.
4. Каким образом ПО стека протоколов определяет, какой пакет инкапсулирован в Ethernet кадр?
5. Каким образом ПО стека протоколов определяет какой протокол транспортного уровня следует использовать при интерпретации IP-дейтаграммы?
6. Для чего необходима фрагментация пакетов?
7. Каким образом задаётся последовательность фрагментов?
8. Как определяется неизвестный MAC-адрес с помощью протокола ARP?

Лабораторная работа № 2
Передача IP-трафика по выделенным линиям

Цель работы: изучить особенности инкапсуляции IP-пакетов в PPP-кадры, работу средств управления линией LCP и конфигурирования сетевых протоколов NCP (IPCP)

Подготовка:

- знать структуру кадра PPP и служебных пакетов LCP, IPCP;
- знать процедуру переговоров LCP для конфигурирования линии;
- знать основные опции пакетов LCP;
- знать основные опции PAP и IPCP.

Задание: выполнить трассировку процессов конфигурирования линии связи, аутентификации, конфигурирования интерфейсов IP, передачи IP-трафика и разъединения протокола PPP с помощью анализатора трафика

Порядок выполнения работы

1. Запустить анализатор трафика, выбрать интерфейс и установить фильтр для отображения PPP-пакетов.
2. Активизировать линию связи (включить модемы выделенной линии либо выполнить дозвон по коммутируемой линии).
3. Выполнить передачу известного файла с ftp-сервера.
4. Остановить запись пакетов и сохранить записанную информацию в файле.
5. Проанализировать последовательность PPP пакетов со схематическим представлением переговоров LCP, PAP, IPCP.

Варианты задания: IP-адрес компьютера, на котором выполняется работа; особенности текущего сеанса протокола PPP (возможно использование собственной трассы).

Дополнительные требования:

1. Отобразить переговоры конфигурирования LCP, PAP, IPCP.
2. Отобразить процесс получения не менее восьми LCP пакетов.
3. Отобразить переговоры завершения связи.
4. Один из LCP пакетов, содержащий не менее 4 опций, представить в исходной (шестнадцатеричной) форме с интерпретацией всех полей.

Содержание отчёта:

- структура кадра PPP, а также использованных в работе LCP, PAP, IPCP пакетов;
- структура использованных в работе опций LCP, PAP, IPCP;
- сохранённая трасса последовательности PPP пакетов;
- схематическое представление переговоров конфигурирования LCP, PAP, IPCP;

- полная интерпретация одного из LCP пакетов по шестнадцатеричному представлению.

Указания по выполнению работы:

Использовать анализатор пакетов Ethereal либо tcpdump (windump). Выбрать интерфейс (PPP interface, dialup adapter). Установить требуемый фильтр (PPP) и запустить запись передаваемых кадров. Остановит процесс записи кадров. Использовать сохранённые кадры для написания отчёта.

Контрольные вопросы:

1. Перечислить основные поля пакета PPP.
2. Перечислить основные фазы PPP-соединения.
3. Перечислить основные запросы для установления соединения.
4. Перечислить основные опции, определяемые для установления соединения.
5. Какие протоколы аутентификации используются в PPP-соединении?
6. Каким образом происходит присвоение IP адреса устройству?
7. Как осуществляется передача информации (данных) в PPP-соединении?
8. Какова процедура завершения в PPP-соединения?

Лабораторная работа № 3
3.1 Передача информации посредством протокола TCP

Цель работы: изучить особенности инкапсуляции UDP дейтаграмм и TCP сегментов в IP- пакеты, процедуры установления соединения («тройное рукопожатие») и параметров передачи данных .

Подготовка:

- знать структуру заголовков TCP и UDP;
- знать процедуру установления TCP соединения ;
- знать основные опции сегмента TCP для передачи данных;
- знать процедуру завершения TCP соединения.;

Задание: выполнить трассировку процессов конфигурирования линии связи, передачи IP-
трафика и разъединения протокола TCP с помощью анализатора трафика.

Порядок выполнения работы

1. Запустить анализатор трафика, выбрать интерфейс и установить фильтр для отображения TCP пакетов.
2. Активизировать линию связи (включить модемы выделенной линии либо выполнить дозвон по коммутируемой линии).
3. Выполнить передачу известного файла с ftp-сервера.
4. Остановить запись пакетов и сохранить записанную информацию в файле.
5. Проанализировать последовательность TCP пакетов со схематическим представлением переговоров (установления соединения, передача данных, завершение соединения).

Варианты задания: IP-адрес компьютера, на котором выполняется работа; оособенности текущего сеанса протокола TCP (возможно использование собственной трассы).

Дополнительные требования:

1. Отобразить переговоры конфигурирования TCP.
2. Отобразить процесс получения не менее восьми TCP пакетов.
3. Отобразить переговоры завершения связи.
4. Один из TCP пакетов представить в исходной (шестнадцатеричной) форме с интерпретацией всех полей.

Содержание отчёта:

- структура сегмента TCP, перечень обслуживаемых прикладных служб;
- структура сегмента UDP, перечень обслуживаемых прикладных служб;
- описание использованных в работе опций TCP;
- сохранённая трасса последовательности TCP пакетов;
- схематическое представление переговоров конфигурирования TCP (процедур соединения, передачи данных, завершения соединения, с указанием использованных кодовых битов);
- полная интерпретация одного из TCP пакетов по шестнадцатеричному представлению.
- полная интерпретация одной из UDP дейтаграмм по шестнадцатеричному представлению.

Указания по выполнению работы:

Использовать анализатор пакетов Ethereal либо tcpdump (windump). Выбрать интерфейс (TCP interface, dialup adapter). Установить требуемый фильтр (TCP) и запустить запись передаваемых пакетов. Остановит процесс записи пакетов. Использовать сохранённые пакеты для написания отчёта.

Примеры анализа пакетов:

Frame 31.

Transmission control protocol (TCP)

- Src Port: 1158, Dst Port: http (80),
- Sequence number: 0 (relative sequence number)
- Header length: 28 bytes
- Flags:0_x0002 (Syn)
- Window size: 16384
- Checksum 0_x91b6 [correct]
- Options (8 bytes):
    1. Maximum segment size: 1460 bytes
    2. Nop
    3. Sack permitted.

Frame 32.

Transmission control protocol (TCP)

- Src Port: http (80), Dst Port: 1158,
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header length: 24 bytes
- Flags:0_x0012 (Syn, Ack)
- Window size: 32768
- Checksum: 0_x21be [correct]
- Options (4 bytes):
    1. Maximum segment size: 576 bytes.

Frame 33.

Transmission control protocol (TCP)

- Src Port: 1158, Dst Port: http (80),
- Sequence number: 1 (relative sequence number)
- Acknowledgment number: 1
- Header length: 20 bytes
- Flags:0_x0010 (Ack)
- Window size: 16704
- Checksum: 0_x74c7 [correct]

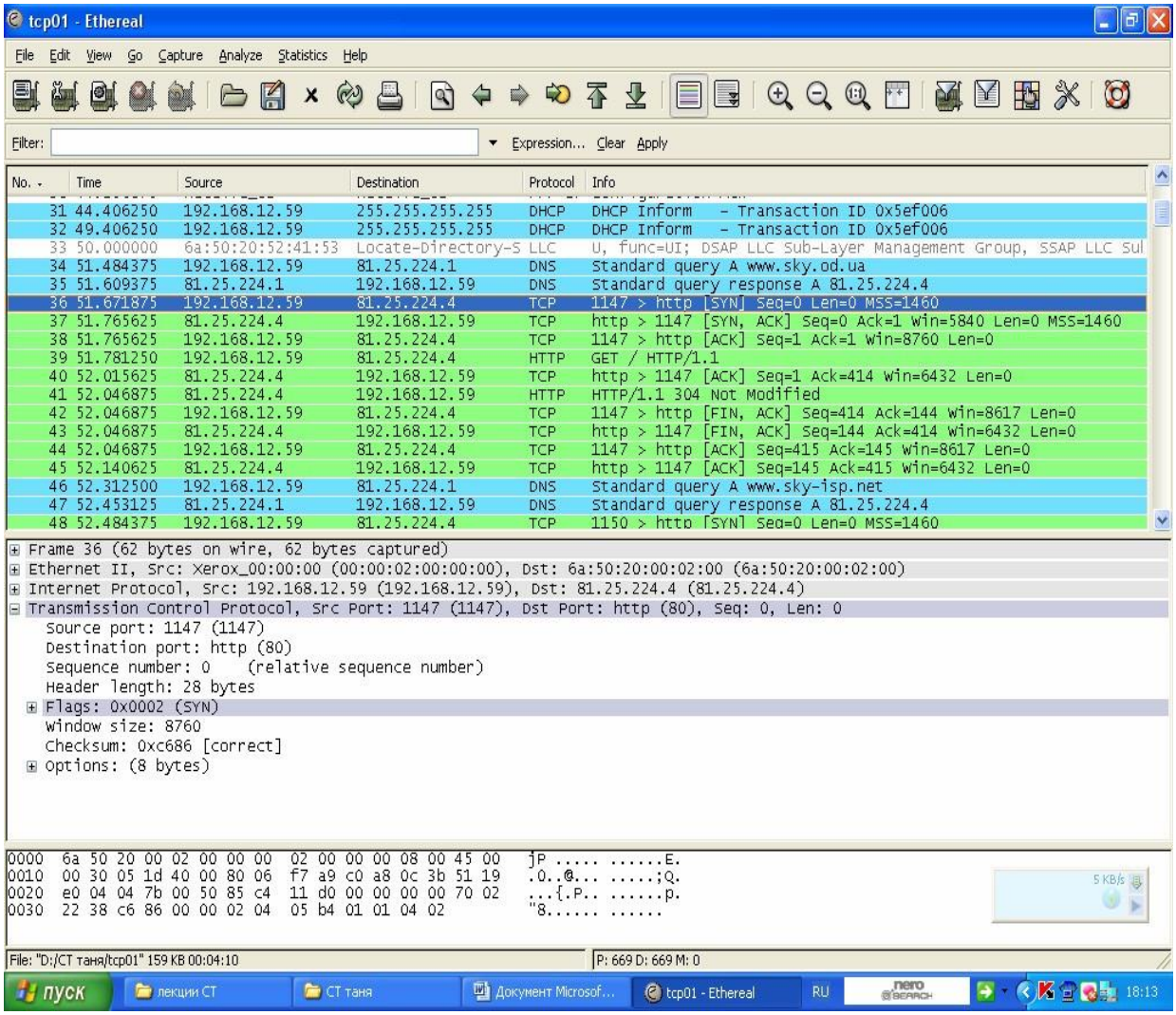
Frame 35.

Transmission control protocol (TCP)

- Src Port: http (80), Dst Port: 1158,
- Sequence number: 1 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header length: 20 bytes
- Flags:0_x0010 (Ack)
- Window size: 33030
- Checksum: 0_x32db [correct].

03 00 03 00 00 00 Destination Address	56 88 20 00 03 00 Source Address	08 00 Type IP	45 Version, Length	00 Dif. Service Field
00 28 Total Length	Cc 02 Identification	10 Flags	00 Fragment offset	32 TTL
06 Protocol	62 b3 Header Checksum	C243391a Source	0a 0a 54 b3 Destination	00 50 Source Port
04 86 Dst Port	08 9a 3f c9 Sequence number	F11663 88 Ack.number	50 Header length	10 Flags

Пример образа экрана Ethereal:



Контрольные вопросы:

1. Перечислите основные поля пакета TCP.
2. Перечислите основные поля дейтаграммы UDP.
3. Перечислить основные фазы TCP-соединения.
4. Какие параметры определяются в процессе установления соединения?
5. Чем идентифицируется логическое TCP-соединение?
6. Опишите работу алгоритма скользящего окна.
7. Для чего служит окно приема?

3.2 Построение таблиц коммутации и покрывающих деревьев

Цель работы: освоить алгоритмы построения таблиц коммутации и покрывающих деревьев.

Подготовка:

- знать структуру кадра Ethernet;
- знать алгоритм работы коммутатора Ethernet;
- знать алгоритм построения покрывающего дерева.

Задание: Выполнить имитацию работы сети с заданными статическими таблицами коммутации в среде моделирующей системы.

Порядок выполнения работы

1. Построить покрывающее дерево.
2. Построить статические таблицы коммутации.
3. Ввести структурную схему сети в моделирующую систему.
4. Ввести таблицы коммутации в моделирующую систему.
5. Выполнить анализ работы сети при заданном трафике; оценить количество потерянных пакетов.

Варианты задания: Структурная схема сети, Приложение 1.

Дополнительные требования:

1. Представить таблицы коммутации всех коммутаторов.
2. Выполнить трассировку доставки не менее чем четырёх кадров.
3. Моделировать трафик между не менее чем четырьмя парами терминальных устройств.
4. Интенсивность трафика 400Кб/с, время работы сети – 10 мин.

Содержание отчёта:

- структурная схема сети
- таблицы коммутации
- трассы доставки пакетов
- описание генераторов трафика
- результаты анализа работы сети – количество потерянных пакетов

Указания по выполнению работы:

Использовать моделирующую систему Opnet. Выбрать коммутаторы Catalyst. Из терминальных устройств: два моделировать как серверы, остальные – как рабочие станции.

Контрольные вопросы:

1. Перечислить основные поля кадра Ethernet.
2. Описать структуру таблицы коммутации.
3. Каким образом коммутатор определяет порт назначения кадра?
4. В каком случае коммутатор выполняет широковещание кадра?

5. Перечислить основные этапы построения покрывающего дерева.
6. Для чего необходим алгоритм построения покрывающих деревьев?
7. Когда коммутатор добавляет запись в динамическую таблицу коммутации?

Подготовка:

Лабораторная работа № 4
4.1Построение статических таблиц маршрутизации

Цель работы: изучить особенности построения и использования статических таблиц IP-
маршрутизации

Подготовка:

- знать структуру заголовка IP-пакета;
- знать бесклассовую система IP-адресации CIDR;
- знать схему доставки IP-пакетов;
- знать структуру таблиц IP-маршрутизации;
- знать алгоритм работы IP-маршрутизатора.

Задание: Выполнить имитацию работы сети с заданными статическими таблицами маршрутизации в среде моделирующей системы.

Порядок выполнения работы

1. Построить статические таблицы маршрутизации.
2. Ввести структурную схему сети в моделирующую систему.
3. Ввести таблицы маршрутизации в моделирующую систему.
4. Выполнить трассировку передачи пакетов между парами терминальных устройств.
5. Выполнить анализ работы сети при заданном трафике; оценить количество потерянных пакетов.

Варианты задания: Структурная схема сети, Приложение 2.

Дополнительные требования:

1. Представить таблицы маршрутизации всех терминальных и сетевых устройств.
2. Выполнить трассировку доставки не менее чем четырёх IP-пакетов.
3. Моделировать трафик между не менее чем четырьмя парами терминальных устройств.
4. Интенсивность трафика 400Кб/с, время работы сети – 10 мин.

Содержание отчёта:

- структурная схема сети
- таблицы маршрутизации
- трассы доставки пакетов
- описание генераторов трафика
- результаты анализа работы сети – количество потерянных пакетов

Указания по выполнению работы:

Использовать моделирующую систему Opnet. Выбрать маршрутизаторы Cisco 2500. Из терминальных устройств: два моделировать как серверы, остальные – как рабочие станции.

Контрольные вопросы:

1. Перечислить основные поля заголовка IP-пакета.
2. Описать структуру таблицы маршрутизации.
3. Каким образом маршрутизатор определяет следующий хоп?
4. Что происходит, если запись о сети отсутствует в таблице маршрутизации?
5. Какие типы метрик используются в таблицах маршрутизации?

4.2 Построение таблиц маршрутизации с помощью протоколов RIP и OSPF

Цель работы: изучить особенности построения таблиц IP-маршрутизации с помощью протоколов динамической маршрутизации RIP и OSPF

Подготовка:

- знать структуру таблиц и алгоритм работы IP-маршрутизатора;
- знать протокол динамической маршрутизации RIP;
- знать протокол динамической маршрутизации OSPF.

Задание: Выполнить имитацию работы протоколов динамической маршрутизации и работу сети, использующей построенные таблицы маршрутизации.

Порядок выполнения работы

1. Построить таблицы маршрутизации с помощью протоколов RIP и OSPF.
2. Ввести структурную схему сети в моделирующую систему.
3. Выполнить трассировку процессов построения таблиц маршрутизации с помощью протоколов RIP и OSPF.
4. Сравнить полученные таблицы маршрутизации с построенными вручную.
5. Выполнить анализ работы сети при заданном трафике; оценить количество потерянных пакетов.

Варианты задания: Структурная схема сети, Приложение 2.

Дополнительные требования:

1. Представить таблицы всех маршрутизазаторов, построенные с помощью протоколов RIP и OSPF.
2. Для одного маршрутизатора представить трассировку процесса построения таблиц с помощью протоколов RIP и OSPF.
3. Моделировать трафик между не менее чем четырьмя парами терминальных устройств.
4. Интенсивность трафика 400Кб/с, время работы сети – 10 мин.

Содержание отчёта:

- структурная схема сети
- таблицы маршрутизации, полученные с помощью протоколов RIP и OSPF
- трассы процессов построения таблиц
- результаты анализа работы сети – количество потерянных пакетов

Указания по выполнению работы:

Использовать моделирующую систему Opnet. Выбрать маршрутизаторы Cisco 2500. Из терминальных устройств: два моделировать как серверы, остальные – как рабочие станции.

Контрольные вопросы:

1. Для чего необходимо применение протоколов динамической маршрутизации?
2. Указать основные этапы работы протокола RIP.
3. Каким образом протокол RIP предотвращает использование устаревших записей?
4. Указать основные этапы работы протокола OSPF.
5. Для чего используются области в протоколе OSPF?
6. Что такое автономная система?
7. Указать основные этапы работы протокола BGP.
8. Каким образом организуется совместная работа нескольких протоколов динамической маршрутизации?

Лабораторная работа № 5
Особенности организации сетей с коммутацией меток

Подготовка:

- формат метки (стека меток) технологии MPLS;
- структура таблиц коммутации меток;
- алгоритм работы LSR/LER маршрутизатора;
- особенности разделения трафика на FEC и построения LSP.

Задачи:

- разделить трафик сети на классы эквивалентности доставки FEC;
- построить пути коммутации меток LSP;
- построить таблицы коммутации меток для LSR/LER.

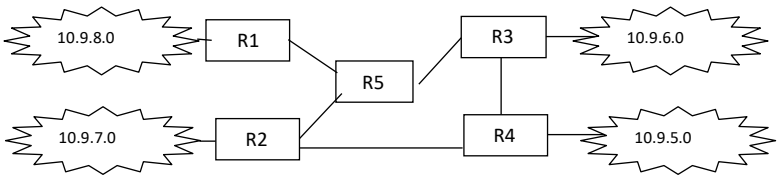
Типовые задания:

1. Для заданной MPLS сети выполнить разделение трафика на FEC.
2. Для заданной сети и FEC построить пути коммутации меток LSP.
3. Для заданной сети и путей коммутации меток LSP построить таблицы коммутации меток всех LSR/LER.
4. Выполнить трассировку прохождения пакетов, используя построенные таблицы коммутации меток.

Примеры решения задач:

Задача № 1.

Выполнить разделение трафика на FEC:



Если не учитывать возможное разделение трафика по требуемому качеству обслуживания, то при выделении FEC рассматривается только пара IP-адресов источника и приёмника. Тогда можно выделить следующие FEC для представленных маршрутизаторов:

- FEC1 (10.9.8.*□10.9.7.*), FEC2 (10.9.8.*□10.9.6.*), FEC3 (10.9.8.*□10.9.5.*);
- FEC4 (10.9.7.*□10.9.8.*), FEC5 (10.9.7.*□10.9.6.*), FEC6 (10.9.8.*□10.9.5.*);
- FEC7 (10.9.6.*□10.9.8.*), FEC8 (10.9.6.*□10.9.7.*), FEC9 (10.9.6.*□10.9.5.*);
- FEC10 (10.9.5.*□10.9.8.*), FEC11 (10.9.5.*□10.9.7.*), FEC12 (10.9.5.*□10.9.6.*).

Задача № 2.

Построить пути коммутации меток LSP:

	10.9.5.*	10.9.6.*	10.9.7.*	10.9.8.*
10.9.5.*	-	R4(1)-R3	R4(1)-R2	R4(2)-R2(1)-R5(1)-R1
10.9.6.*	R3(1)-R4	-	R3(2)-R4(3)-R2	R3(2)-R5(2)-R1
10.9.7.*	R2(3)-R4	R2(3)-R5(2)-R3	-	R2(4)-R5(3)-R1
10.9.8.*	R1(5)-R5(3)-R3(4)-R4	R1(6)-R5(4)-R3	R1(7)-R5(4)-R2	-

Заметим, что при назначении меток, указанных в скобках, использован уникальный выбор метки для каждого FEC в пределах маршрутизатора. Количество используемых меток можно сократить, если использовать уникальные метки только в пределах одного и того же интерфейса. Выполнить указанное назначение меток самостоятельно.

Задача № 3.

Построить таблицы коммутации меток для
LSR/LER: R1:

Входной интерфейс	Входная метка	Выходной интерфейс	Выходная метка
i10.9.8(□10.9.5)	-	iR5	5
i10.9.8(□10.9.6)	-	iR5	6
i10.9.8(□10.9.7)	-	iR5	7
iR5	1	i10.9.8	-
iR5	2	i10.9.8	-
iR5	3	i10.9.8	-

R2:

Входной интерфейс	Входная метка	Выходной интерфейс	Выходная метка
i10.9.7(□10.9.5)	-	iR4	3
i10.9.7(□10.9.6)	-	iR5	3
i10.9.7(□10.9.8)	-	iR5	4
iR4	1	i10.9.7	-
iR4	3	i10.9.7	-
iR5	4	i10.9.7	-
iR4	2	iR5	1

R3:

Входной интерфейс	Входная метка	Выходной интерфейс	Выходная метка
i10.9.6(□10.9.5)	-	iR4	1
i10.9.6(□10.9.7)	-	iR4	2
i10.9.6(□10.9.8)	-	iR5	2
iR4	1	i10.9.6	-
iR5	2	i10.9.6	-
iR5	4	i10.9.6	-
iR5	3	iR4	4

R4:

Входной интерфейс	Входная метка	Выходной интерфейс	Выходная метка
i10.9.5(□10.9.6)	-	iR3	1
i10.9.5(□10.9.7)	-	iR2	1
i10.9.5(□10.9.8)	-	iR2	2
iR3	1	i10.9.5	-
iR2	3	i10.9.5	-
iR3	4	i10.9.5	-
iR3	2	iR2	3

R5:

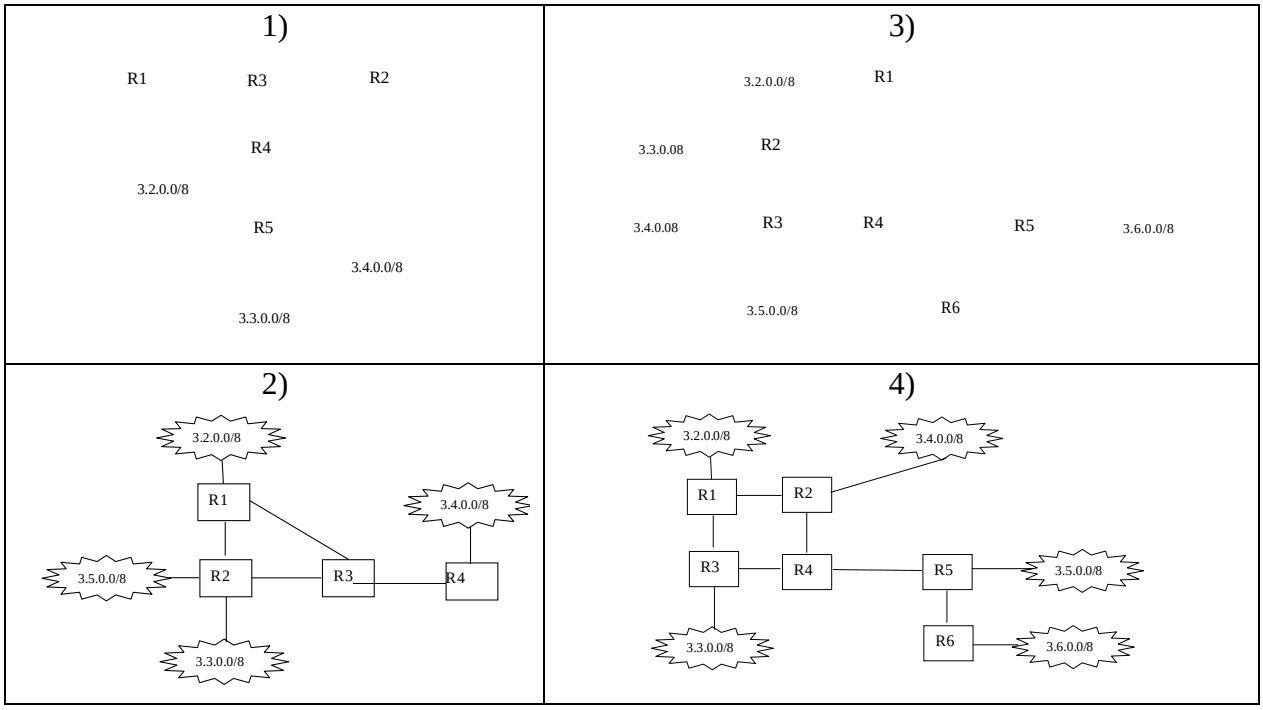
Входной интерфейс	Входная метка	Выходной интерфейс	Выходная метка
iR2	1	iR1	1
iR3	2	iR1	2
iR2	3	iR3	2
iR2	4	iR1	3
iR1	5	iR3	3
iR1	6	iR4	4
iR1	7	iR2	2

Задача № 4.

Выполнить трассировку прохождения пакетов:

10.9.8.115□10.9.5.47:
10.9.8.115□
R1 (строка 1: метка 5, интерфейс iR5) □ R5 (строка 5: метка 3, интерфейс iR3) □ R3 (строка 7: метка 4, интерфейс iR4) □
R4 (строка 6: интерфейс i10.9.5) □10.9.5.0□10.9.5.47

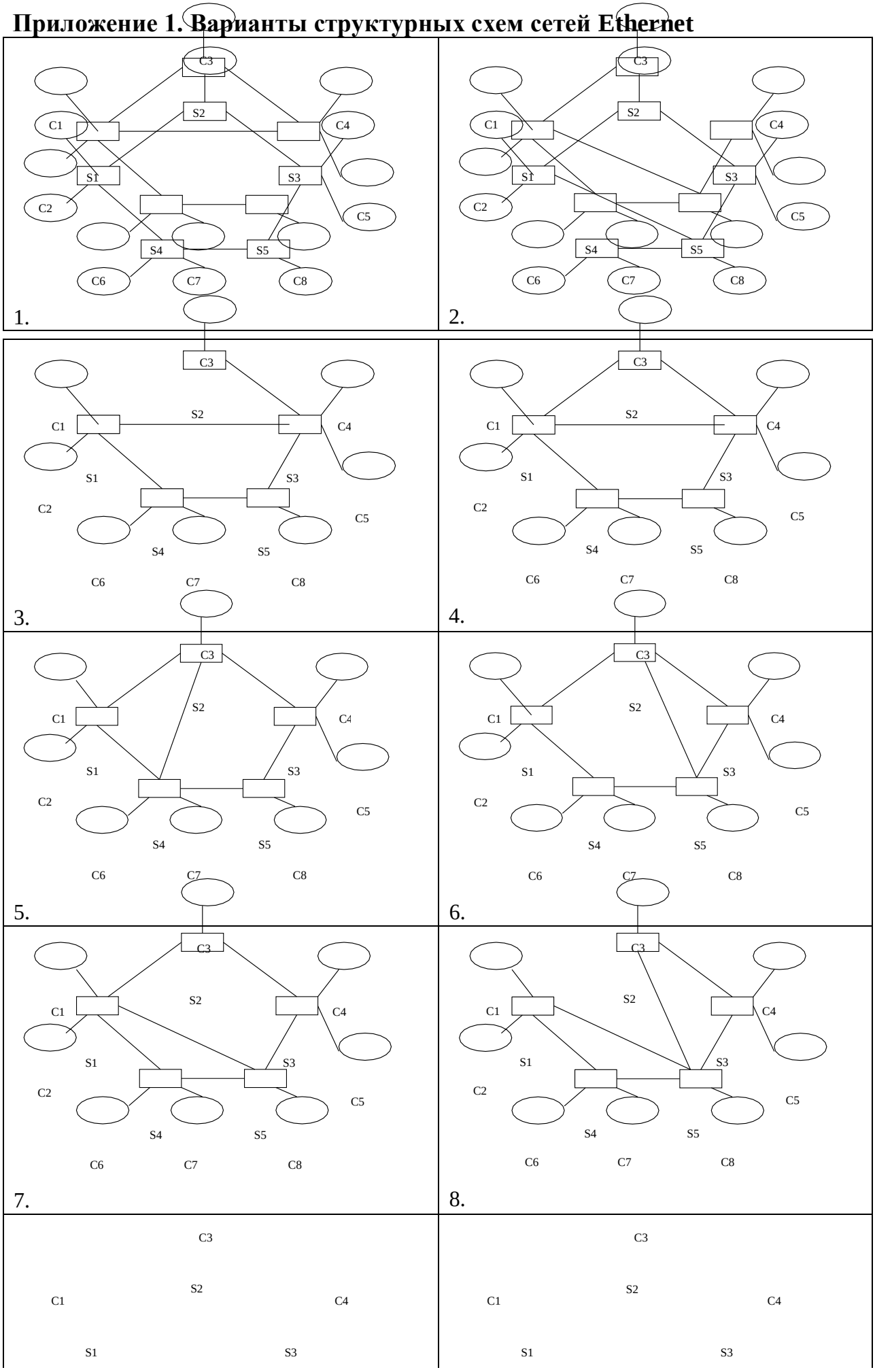
Варианты заданий для самостоятельных упражнений:



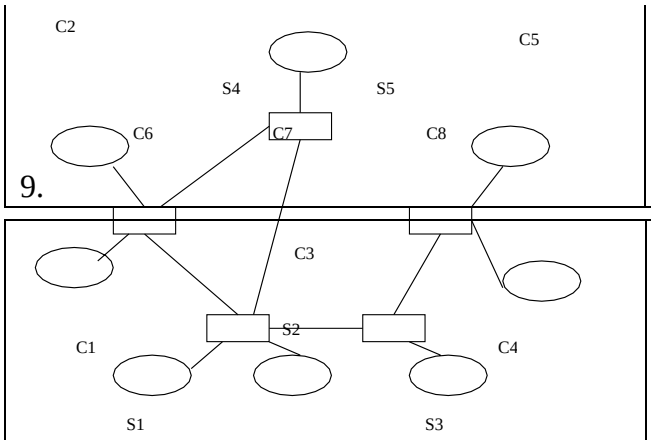
Контрольные вопросы:

1. Для чего необходимо применение технологии коммутации меток?
2. Описать формат заголовка MPLS.
3. Описать структуру таблицы коммутации меток.
4. Что такое путь коммутации меток LSP?
5. Что такое класс эквивалентности доставки FEC?
6. Каким образом выполняется назначение меток?
7. Для чего применяется стек меток в технологии MPLS?

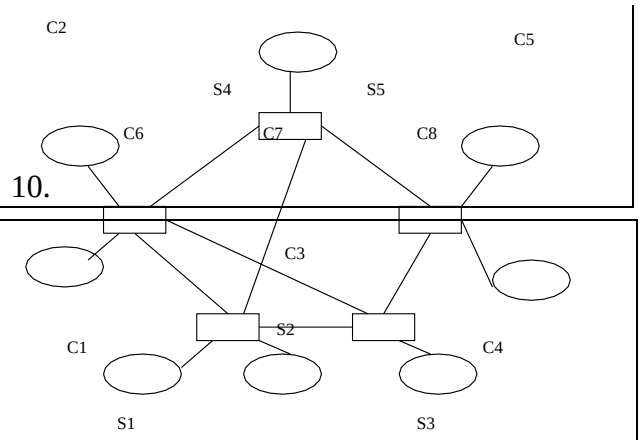
Приложение 1. Варианты структурных схем сетей Ethernet



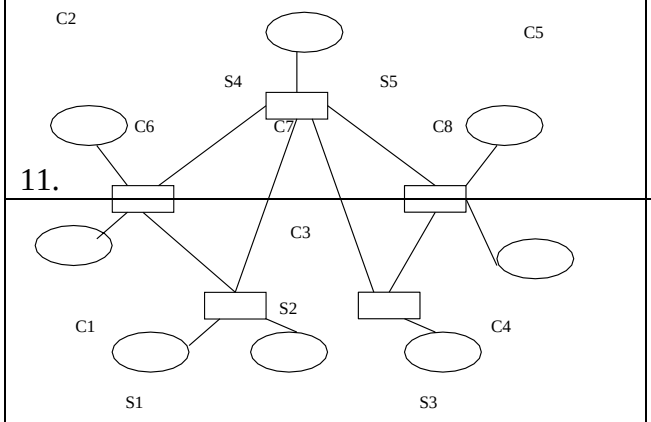
9.



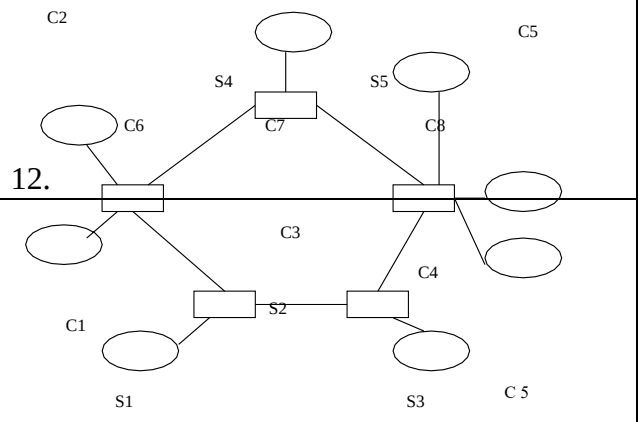
10.



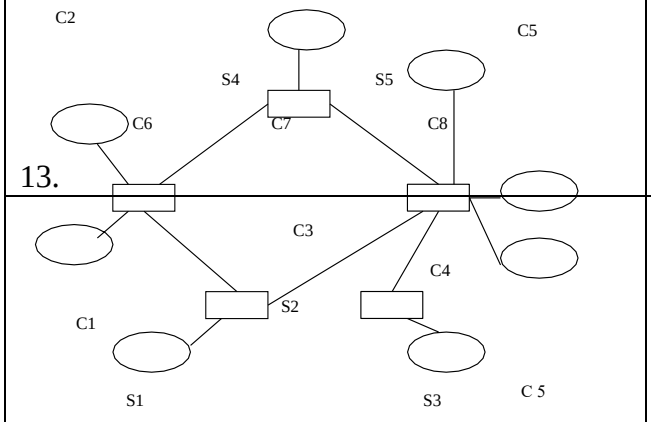
11.



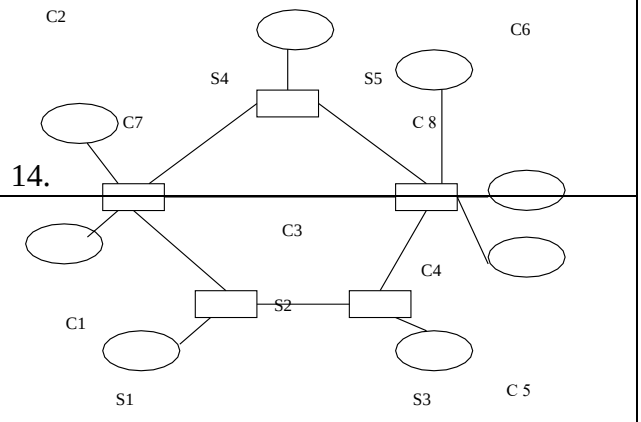
12.



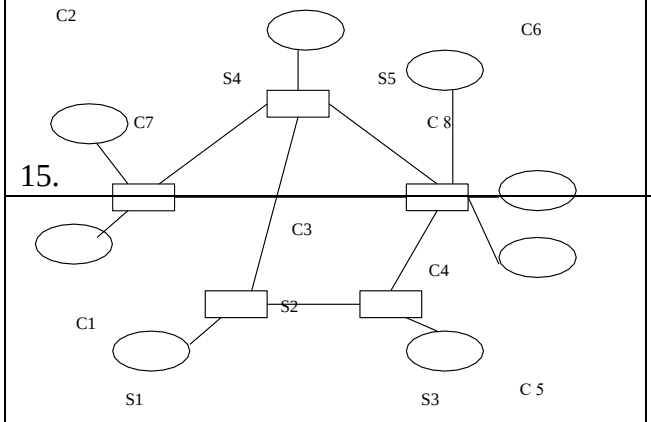
13.



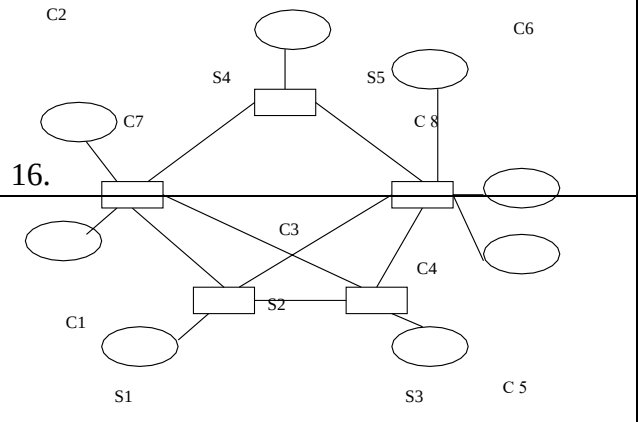
14.



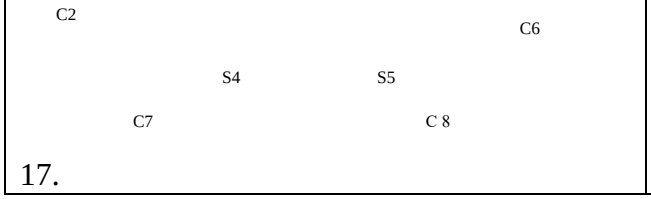
15.



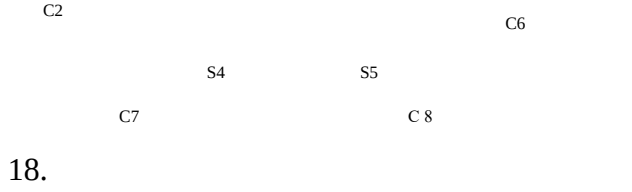
16.

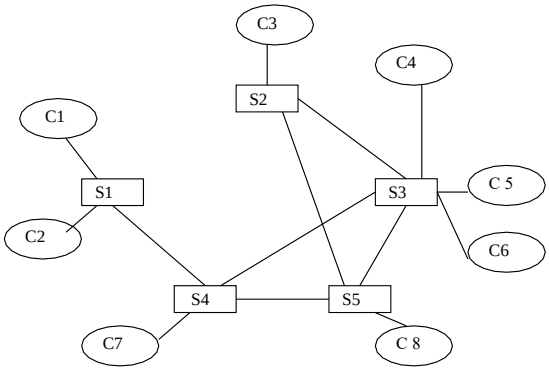


17.

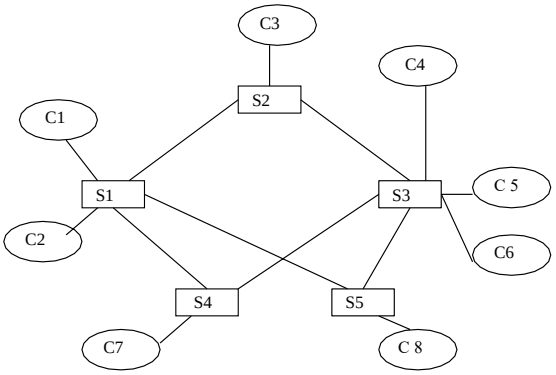


18.

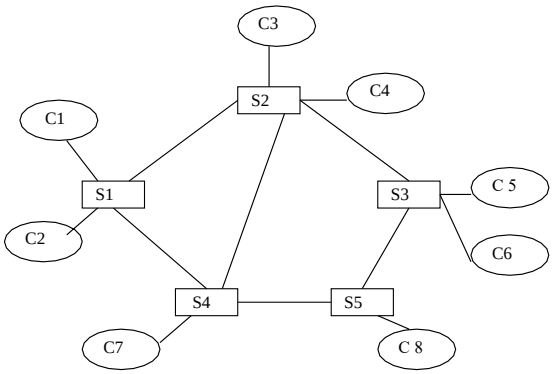




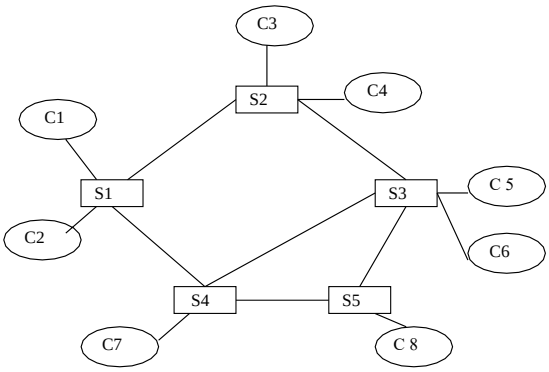
19.



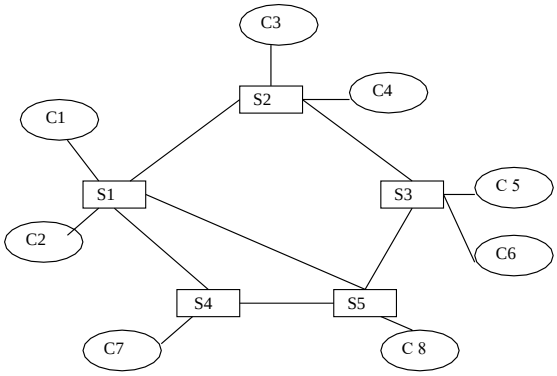
20.



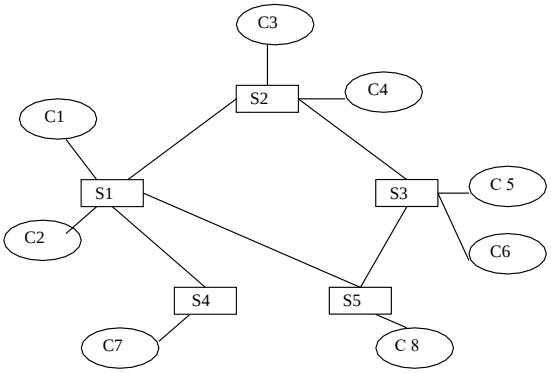
21.



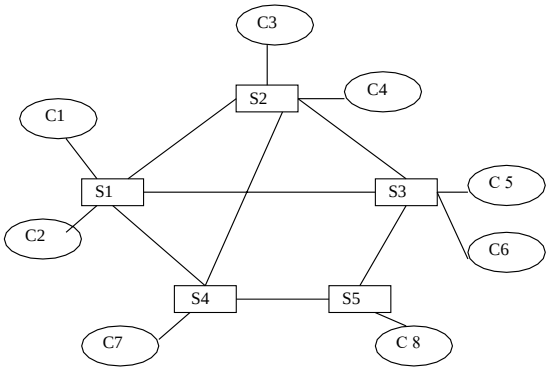
22.



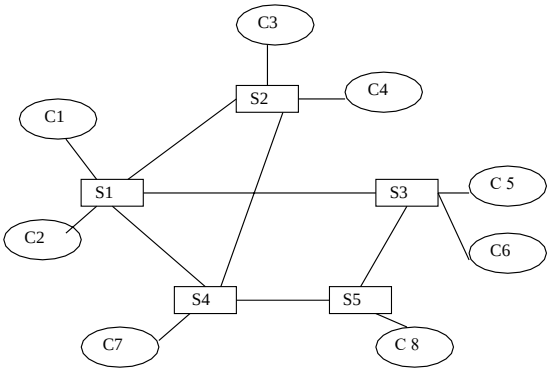
23.



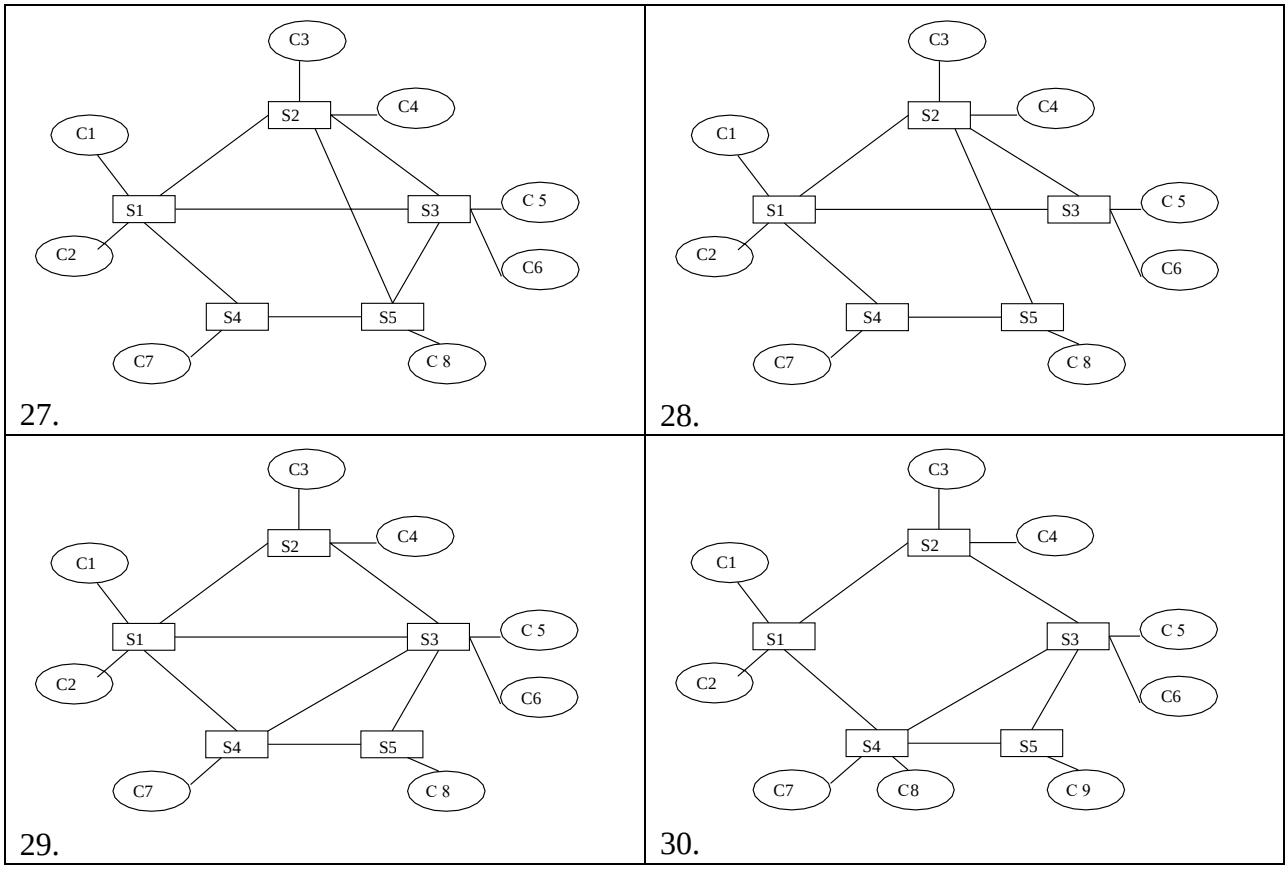
24.



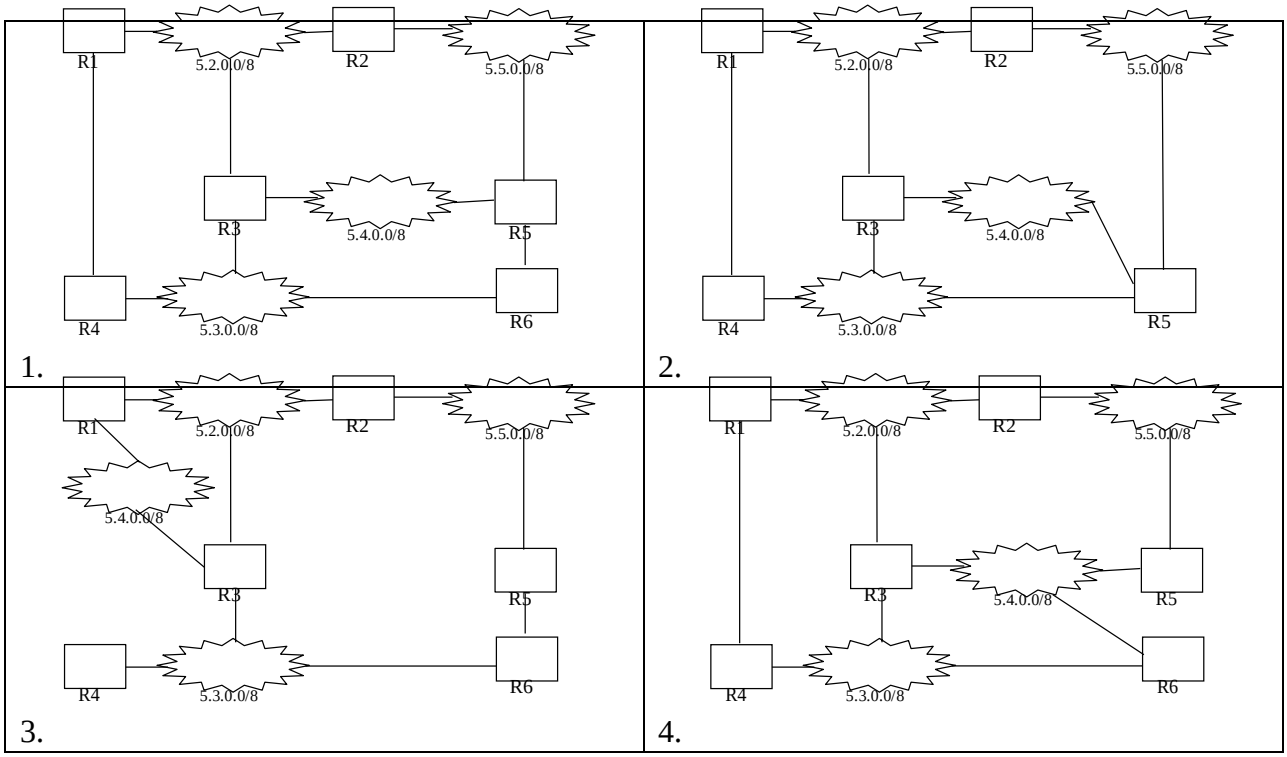
25.



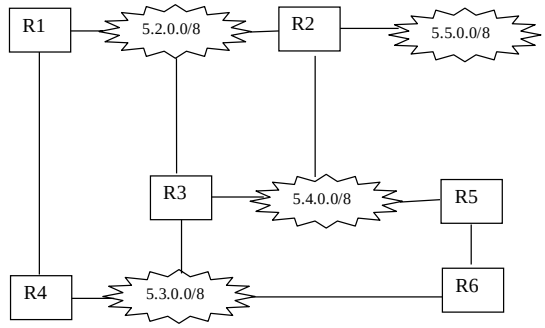
26.



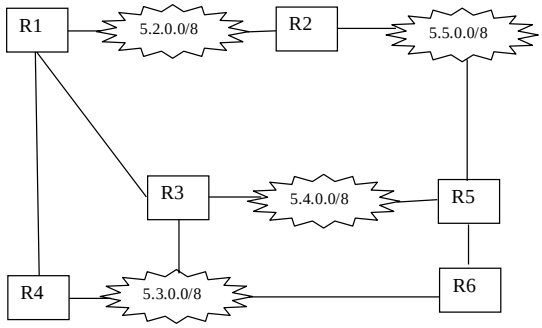
Приложение 2. Варианты структурных схем IP-сетей



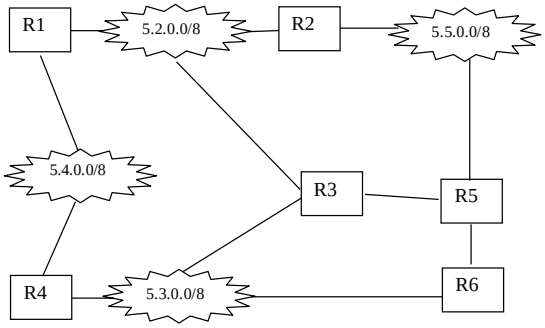
5.



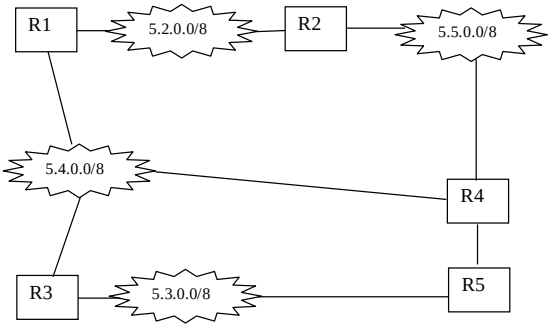
6.



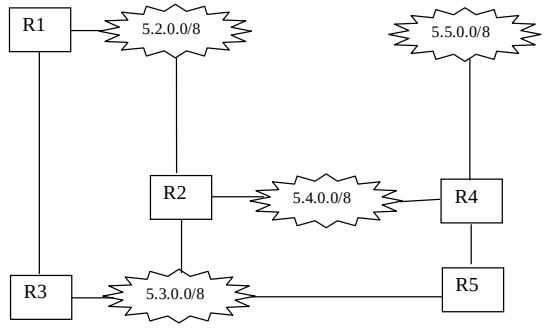
7.



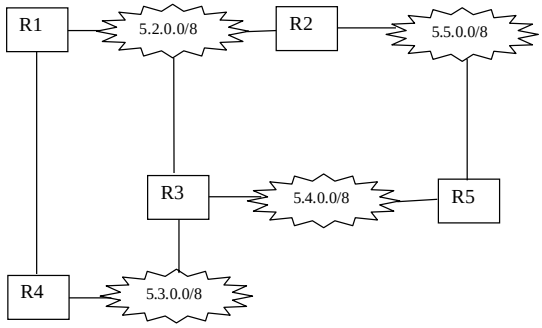
8.



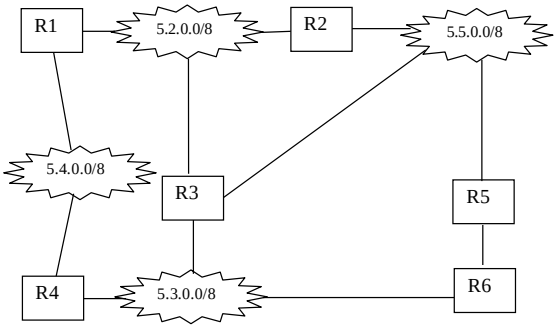
9.



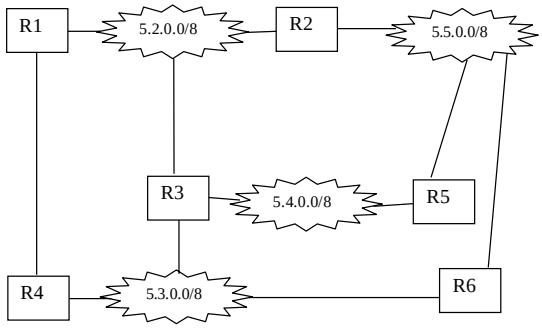
10.



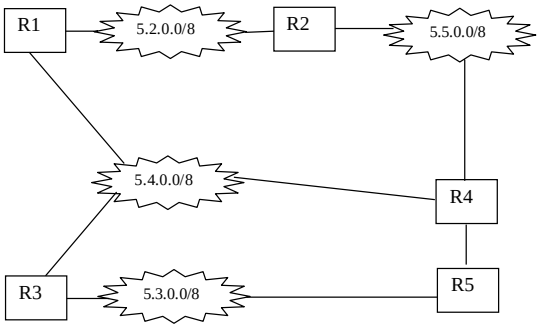
11.



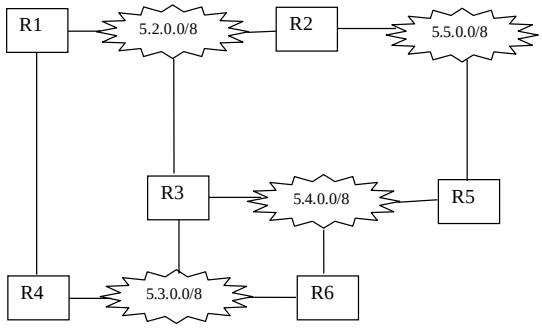
12.



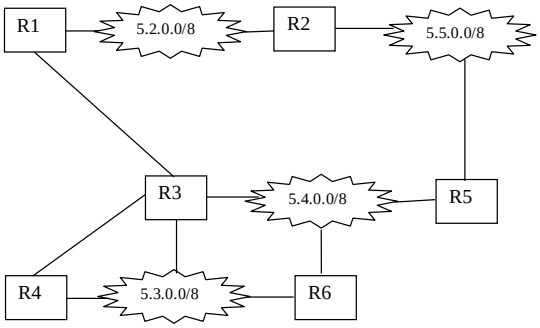
13.



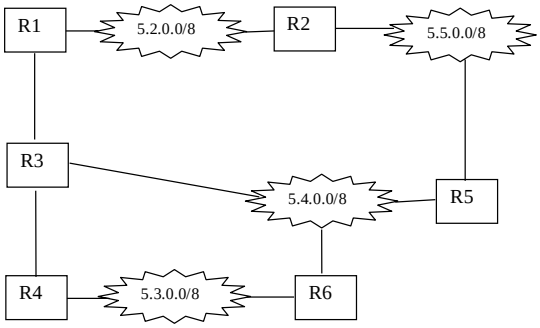
14.



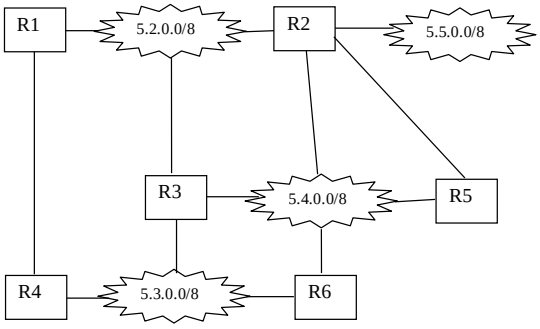
15.



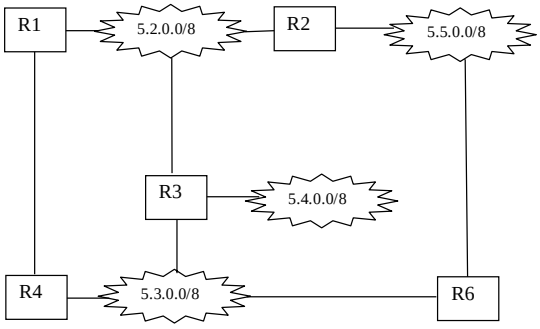
16.



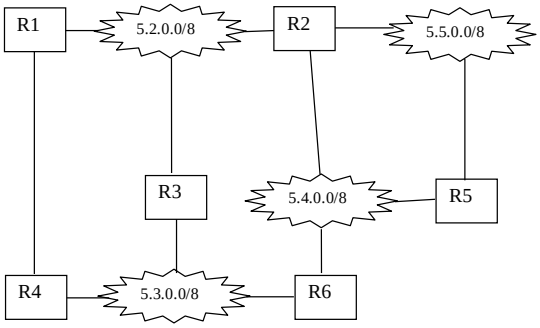
17.



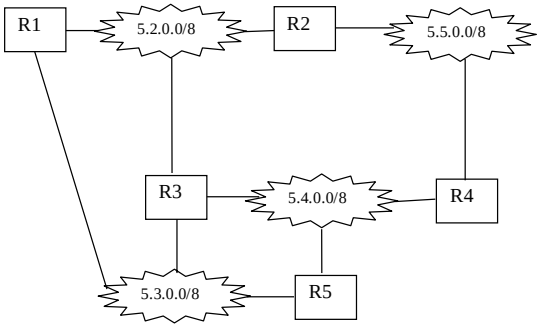
18.



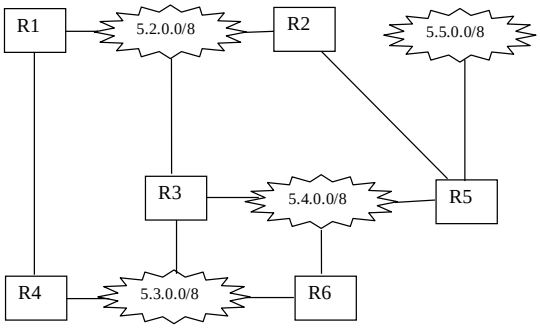
19.



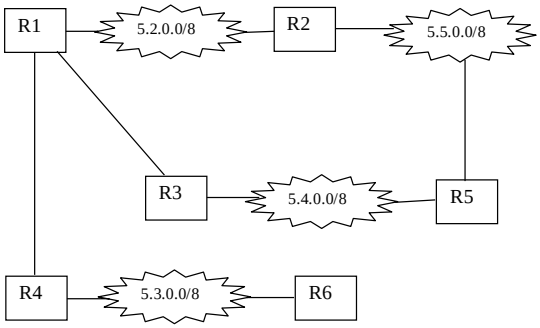
20.



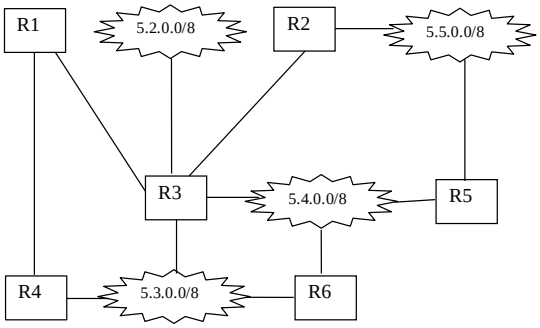
21.



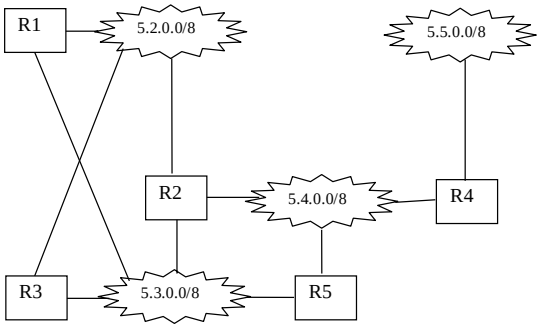
22.



23.

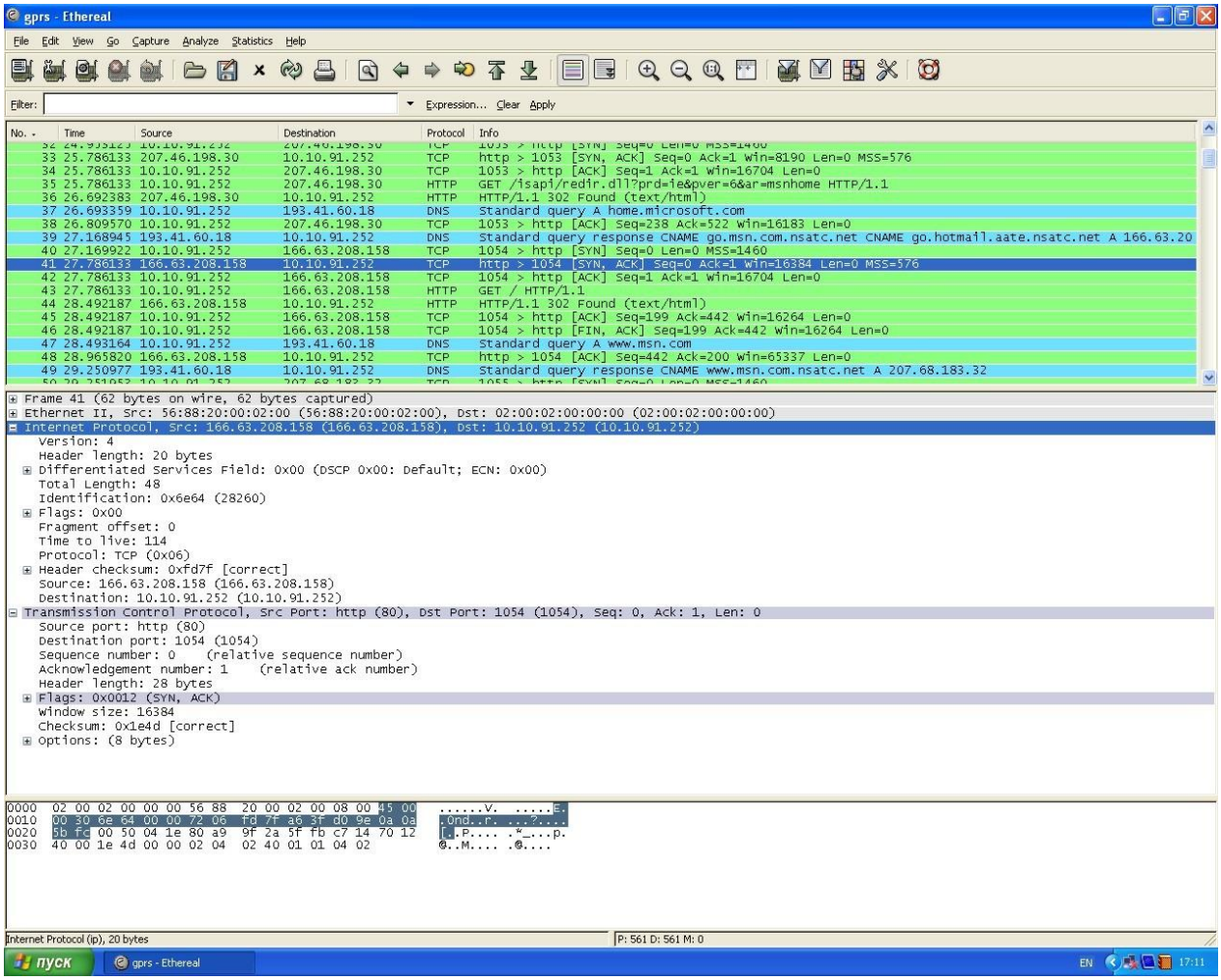


24.



Приложение 3. Краткое описание анализатора трафика Ethereal

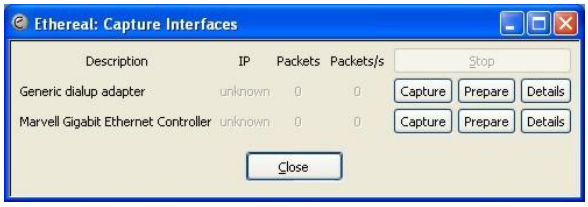
Программа Ethereal (http://www.ethereal.com) позволяет прослушивать выбранный сетевой интерфейс с динамическим отображением передаваемых пакетов, записать последовательность пакетов в указанный файл, проанализировать содержимое пактов. Программа обеспечивает подсчет количества переданных пакетов по каждому из указанных протоколов. Возможна фильтрация трафика для отображения и сохранения выбранных типов пакетов, а также анализ ранее сохранённой в файле трассы. Далее приведен пример образа экрана Ethereal:



В верхней части экрана отображен фрагмент последовательности пакетов с их кратким описанием: номер (No.), время поступления (Time), источник (Source), назначение (Destination), протокол (Protocol), краткая информация (Info). В средней части экрана представлены допустимые шаблона интерпретации заголовков пакета в соответствии с инкапсулированными протоколами. В настоящем примере интерпретированы IP и TCP заголовки текущего пакета. В нижней части экрана представлен шестнадцатеричный дамп пакета: в первой колонке указаны смещения от начала пакета, во второй – шестнадцатеричный дамп, в третьей – символьная интерпретация.

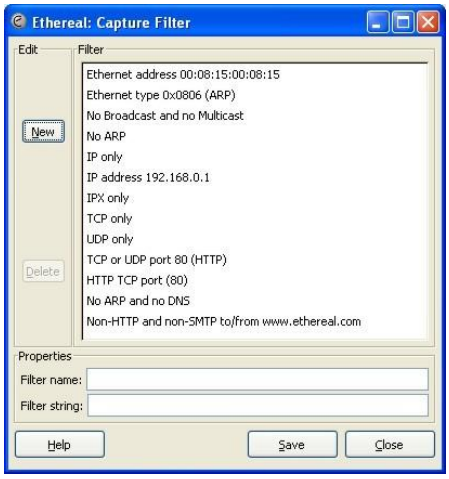
Для записи передаваемой информации служит раздел меню Захват (Capture).

Возможно простое прослушивание указанного сетевого интерфейса с помощью кнопок окна пункта меню Интерфейсы (Interfaces):

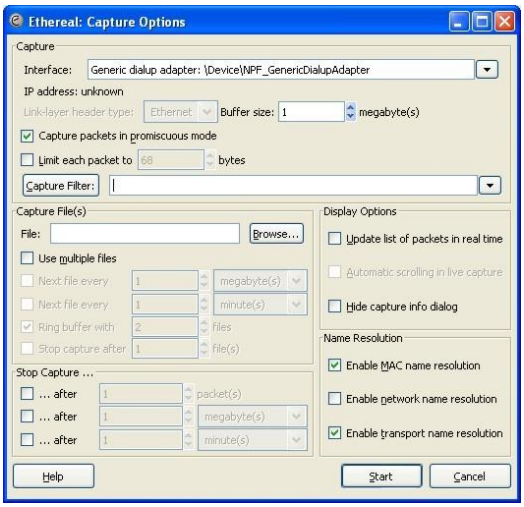


В указанном примере доступны два интерфейса: Адаптер коммутируемой связи (Generic dialup adapter) и Контроллер сети Ethernet (Marvell Gigabit Ethernet Controller). Запуск прослушивания выполняется нажатием соответствующей кнопки Захват (Capture). После этого появляется окно со статистикой полученных пакетов; завершение прослушивания выполняется нажатием кнопки Стоп (Stop). Записанная последовательность пакетов может быть сохранена в файле с помощью пунктов раздела меню Файл (File); этот раздел меню позволяет также загрузить ранее сохранённую последовательность пакетов.

Трафик реальных сетей может быть весьма интенсивным, что приводит к большим объемам сохранённых последовательностей пакетов. В программе Ethereal предусмотрена возможность фильтрации, в этом случае записываются только пакеты, удовлетворяющие указанному фильтру. В простейшем случае фильтр задаёт имя протокола; возможно формирование более сложных фильтров указанием адресов отправителя либо получателя, номеров портов и другой информации. Фильтры создаются в окне пункта меню Фильтры захвата (Capture Filters):



Для совместного указания интерфейса и фильтра служит пункт меню Опции (Options):



Приложение 4. Краткое описание моделирующей системы Opnet

Система Opnet (http://www.opnet.com) позволяет ввести в графическом редакторе структурную схему сети. Графическими элементами являются сетевые устройства (коммутаторы, маршрутизаторы), линии связи, а также терминальные устройства: серверы и рабочие станции. Предусмотрено большое число моделей реальных устройств в библиотеке компонентов моделирующей системы. Кроме того, в дополнительных текстовых окнах вводятся параметры конфигурации устройств. Например, MAC- и IP- адреса, таблицы коммутации и маршрутизации, перечень используемых протоколов.

Для терминальных устройств возможно описание трафика сети. В генераторах трафика указываются прикладные протоколы ftp, http, интенсивность трафика, длины передаваемых пакетов, адреса назначения.

Система Opnet не предоставляет средства непосредственной визуализации телекоммуникационных процессов. Однако, возможна проверка работоспособности сети с помощью имитационного моделирования, представленного итоговыми результатами работы сети за указанный период реального времени, собранными с помощью специальных вычислительных элементов модели.

Целостность моделируемой сети и гарантированная доставка пакетов может быть косвенно оценена нулевым количеством потерянных пакетов. Возможна оценка дополнительных характеристик, таких как трафик сети, время доставки пакета.

Библиографический список

1. Моделирование систем [Текст] : учебное пособие / И. А. Елизаров [и др.]. - Старый Оскол : ТНТ, 2013. – 136 с.

2. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

1. Технологии коммутации и маршрутизации в локальных компьютерных сетях [Текст] : учебное пособие / под общ.ред. А. В. Пролетарского. - Москва : Изд - во МГТУ им. Н. Э. Баумана, 2013. - 389, [3] с.

2. Отечественные телекоммуникационные системы [Текст] : учебное пособие для вузов / Ю. К. Шарипов, В. К. Кобляков. - 3-е изд., перераб. и доп. - М. : Логос, 2005. – 832 с.

3. Системы и сети передачи информации [Электронный ресурс] : учебное пособие / Ю. Ю. Громов, И. Г. Карпов, Г. Н. Нурутдинов. - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2012. - 128 с. – Режим доступа: biblioclub.ru