Лабораторная работа №3.
«Инкапсуляция. Расшифровка полей заголовков канального и сетевого уровня в Wireshark»
Теоретические основы

1. Инкапсуляция

Важным процессом при передаче данных является инкапсуляция данных. Передаваемое сообщение, сформированное приложением, проходит три верхних сетенезависимых уровня и поступает на транспортный уровень, где делится на части, и каждая часть инкапсулируется (помещается) в сегмент данных (рис. 1). В заголовке сегмента содержится номер протокола прикладного уровня, с помощью которого подготовлено сообщение, и номер протокола, который будет обрабатывать данный сегмент.

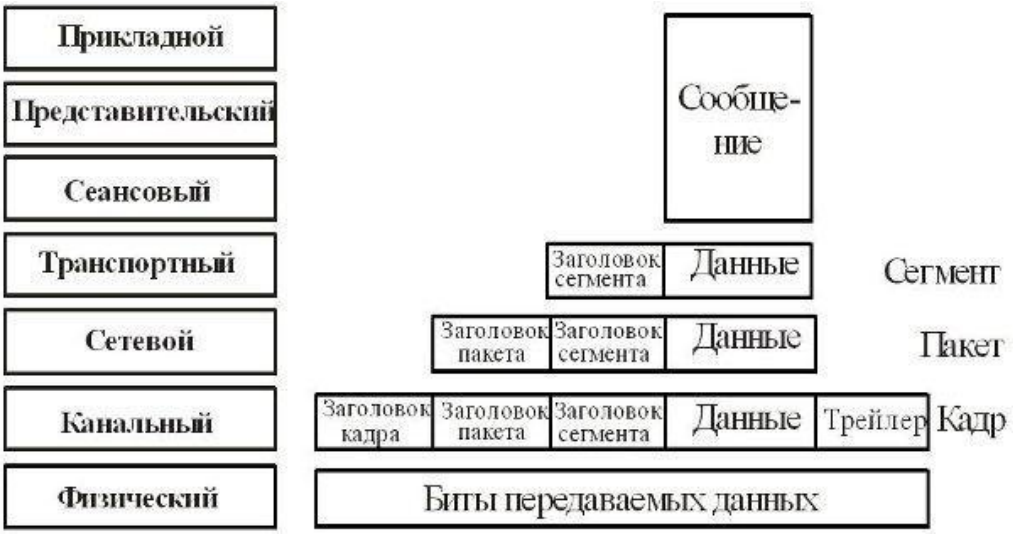

Рис. 1.

На сетевом уровне сегмент инкапсулируется в пакет данных, заголовок которого содержит, кроме прочего, IP-адреса отправителя информации (источника) и получателя (назначения).

На канальном уровне пакет инкапсулируется в кадр или фрейм данных, заголовок которого содержит MAC-адреса узла передатчика и приемника, а также другую информацию. Кроме того, на этом уровне добавляется трейлер (концевик) кадра, содержащий информацию, необходимую для проверки правильности принятой информации. Таким образом, происходит обрамление данных заголовками со служебной информацией, т. е. инкапсуляция данных.

2. Канальный уровень

На канальном уровне работает технология Ethernet. Существует несколько стандартов формата кадра Ethernet. На практике в оборудовании Ethernet используется только один формат кадра, а именно — кадр Ethernet II. Этот формат представлен на рис. 2.

6 байт	6 байт	2 байта	46–1500 байт	4 байта
DA	SA	T	Данные	FCS

Рис.2. Формат кадра Ethernet II

DA (Destination Address) — MAC-адрес узла назначения;

SA (Source Address) — MAC-адрес узла отправителя.

Поле **T** (Type, или EtherType) содержит условный код протокола верхнего уровня, данные которого находятся в поле данных кадра, например шестнадцатеричное значение 08-00 соответствует протоколу IP.

Поле **данных** может содержать от 46 до 1500 байт. Если длина пользовательских данных меньше 46 байт, то это поле дополняется до минимального размера байтами заполнения.

Данными на канальном уровне считается всё, что находится после поля T, в том числе заголовок следующего, сетевого, уровня. Это значит, что устройство сетевого уровня (коммутатор) эту часть не рассматривает.

Поле **контрольной последовательности кадра** (Frame Check Sequence, FCS) состоит из 4 байт контрольной суммы. Это значение вычисляется по алгоритму CRC-32. Большинство интерфейсов Ethernet не предоставляют значение FCS для Wireshark.

Далее приведена распечатка значений полей заголовка *канального* уровня одного из реальных IP-пакетов, захваченных в сети Ethernet средствами анализатора протоколов сетевого монитора Wireshark. Программа представляет числовые коды полей в виде, более удобном для чтения, и интерпретирует некоторые результаты.

Ethernet II, Src: Chongqin_ea:24:31 (8c:c8:4b:ea:24:31), Dst: Routerbo_dc:46:95 (cc:2d:e0:dc:46:95)

Destination: Routerbo_dc:46:95 (cc:2d:e0:dc:46:95)

Source: Chongqin_ea:24:31 (8c:c8:4b:ea:24:31)

Type: IPv4 (0x0800)

3. Сетевой уровень

На сетевом уровне работает протокол IP. Протокол IP относится к протоколам без установления соединений, поддерживая обработку каждого IP-пакета как независимой единицы обмена, не связанной с другими пакетами. В протоколе IP нет механизмов, обычно применяемых для обеспечения достоверности конечных данных. Если во время продвижения пакета происходит какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для ее исправления. Например, если на промежуточном маршрутизаторе пакет был отброшен из-за ошибки по контрольной сумме, то модуль IP не пытается заново послать потерянный пакет. Другими словами, протокол IP реализует политику доставки «по возможности».

Изучая назначение каждого поля заголовка IP-пакета (рис. 1), мы не только получаем формальные знания о структуре пакета, но и знакомимся с основными функциями протокола IP.

Рис. 1. Структура заголовка IP-пакета

Поле **номера версии** занимает 4 бита и идентифицирует версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4), хотя все чаще встречается и новая версия (IPv6). Значение **длины заголовка** IP-пакета также занимает 4 бита и измеряется в 32-битных словах. Обычно заголовок имеет длину в 20 байт (пять 32-битных слов), но при добавлении некоторой служебной информации это значение может быть увеличено за счет дополнительных байтов в поле параметров. Наибольшая длина заголовка составляет 60 байт.

Поле **типа сервиса** имеет и другое, более современное название – **байт дифференцированного обслуживания** (Differentiated Services Field), или DS-байт. Первые три бита содержат значение **приоритета (PR)** пакета: от самого низкого – 0 до самого высокого – 7. Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь.

Следующие три бита определяют критерий выбора маршрута. Если для бита D (Delay – задержка) установлено значение 1, то маршрут должен выбираться для минимизации задержки доставки данного пакета, установленный бит T (Throughput – пропускная способность) – для максимизации пропускной способности, а бит R (Reliability – надежность) – для максимизации надежности доставки.

Оставшиеся два бита служат для реализации дополнительной функции - явном уведомлении о перегруженности (Explicit Congestion Notification, ECN). Поддерживающие расширение ECN маршрутизаторы могут сигнализировать о начале заторов, устанавливая биты в заголовке IP, а не удаляя пакеты:

00: поток, не поддерживающий ECN, англ. Not-ECN-Capable Transport (ECT)

01 или 10: поток, поддерживающий ECN, англ. ECN-Capable Transport (Not-ECT)

11: подтвержденная перегрузка, англ. Congestion Experienced (CE)

Поле **общей длины (Total Length)** занимает 2 байта и характеризует общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65535 байт, но в большинстве компьютеров и сетей столь большие пакеты не используются. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной 1500 байт, умещающиеся в поле данных кадра Ethernet. В стандартах TCP/IP предусматривается, что все

хосты должны быть готовы принимать пакеты длиной вплоть до 576 байт (независимо от того, приходят они целиком или фрагментами).

В поле **Идентификатор пакета**, длина которого 2 байта, указывается номер каждого пересылаемого пакета IP. Этот номер увеличивается каждый раз на 1 при очередной посылке пакета, за исключением пересылки фрагментированных IP-пакетов, в которых значение в данном поле одинаковое для всех фрагментов. Для идентификации фрагментов используются поля **Флаги** и **Смещение фрагмента**.

Флаги занимают 3 бита и содержат признаки, связанные с фрагментацией. Установленный в 1 бит DF (Do not Fragment – не фрагментировать) запрещает маршрутизатору фрагментировать данный пакет, а установленный в 1 бит MF (More Fragments – больше фрагментов) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле смещения фрагмента занимает 13 бит и задает смещение в байтах поля данных этого фрагмента относительно начала поля данных исходного фрагментирующего пакета. Используется при сборке/разборке фрагментов пакетов. Смещение должно быть кратно 8 байтам.

Поле времени жизни (Time To Live, TTL) занимает один байт и используется для задания предельного срока, в течение которого пакет может перемещаться по сети. Время жизни пакета измеряется в переходах между устройствами уровня 3 и выше и задается источником. По истечении каждой секунды пребывания на каждом из маршрутизаторов, через которые проходит пакет во время своего «путешествия» по сети, из его текущего времени вычитается единица; единица вычитается и в том случае, если время пребывания – менее секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше, чем за одну секунду, то время жизни можно интерпретировать как максимальное число транзитных узлов, которые разрешено пройти пакету. Если значение поля времени жизни становится нулевым до того, как пакет достигает получателя, то пакет уничтожается. Таким образом, время жизни является своего рода часовым механизмом самоуничтожения пакета.

Поле протокола верхнего уровня занимает 1 байт и содержит идентификатор, указывающий, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета. Значения идентификаторов для разных протоколов приводятся в документе RFC 1700, доступном по адресу http://www.iana.org. Например, 6 означает, что в пакете находится сообщение протокола TCP, 17 – протокола UDP, 1 – протокола ICMP.

Контрольная сумма заголовка занимает 2 байта (16 бит) и рассчитывается без учета поля данных, т.е. только по заголовку IP-пакета. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, поле времени жизни), контрольная сумма проверяется и повторно рассчитывается на каждом маршрутизаторе и конечном узле как дополнение к сумме всех 16-битных слов заголовка. Проверка контрольной суммы может быть также отключена (validation disabled).

Поля IP-адресов источника (Source IP Address) и приёмника (Destination IP Address) имеют одинаковую длину – 32 бита.

Поле **опций** является необязательным и используется обычно только при отладке сети. Это поле состоит из нескольких подполей одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут, по которому маршрутизаторы должны направлять

данный пакет (то есть выполнять маршрутизацию от источника), регистрировать проходимые пакетом маршрутизаторы или помещать данные системы безопасности и временные отметки. Так как число подполей в поле параметров может быть произвольным, то в конце заголовка должно быть добавлено несколько нулевых байтов для **выравнивания** заголовка пакета по 32-битной границе.

Далее приведена распечатка значений полей заголовка *сетевого* уровня одного из реальных IP-пакетов, захваченных в сети Ethernet средствами анализатора протоколов сетевого монитора Wireshark. Программа представляет числовые коды полей в виде, более удобном для чтения, и интерпретирует некоторые результаты на английском языке.

Internet Protocol Version 4, Src: 10.255.82.47, Dst: 93.184.220.29
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 389
Identification: 0x58e2 (22754)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x098d [validation disabled]
[Header checksum status: Unverified]
Source: 10.255.82.47
Destination: 93.184.220.29

Ход работы

1. Откройте программу Wireshark и начните захват кадров.
2. Прекратите захват кадров. Выделите один кадр, использующий как протокол сетевого уровня IP версии 4 (т.е. не ARP, у которого своя структура пакета, и не IPv6).
3. На панели декодера протоколов, нажимая указателем мыши на символ «>», отобразите информацию о полях заголовка канального уровня (Ethernet II) с требуемым уровнем детализации. Скопируйте распечатку значений полей (Копировать – Все видимые пункты выбранного дерева) в отчёт.
4. Пользуясь рисунком и методическими указаниями, проинтерпретируйте на русском языке поля заголовков канального уровня.
5. На панели декодера протоколов, нажимая указателем мыши на символы «>», отобразите информацию о полях заголовка сетевого уровня (Internet Protocol version 4) с требуемым уровнем детализации. Скопируйте распечатку значений полей (Копировать – Все видимые пункты выбранного дерева) в отчёт.

6. Пользуясь рисунком и методическими указаниями, проинтерпретируйте на русском языке поля заголовков сетевого уровня.