ПАКЕТНАЯ ПЕРЕДАЧА ДАННЫХ

3.0.1.1

Исторически так сложилось, что компьютерные сети имеют последовательную природу. Объяснить это можно тем, что реализовать передачу данных на сравнительно больши'е расстояния в параллельном виде значительно сложнее, чем в последовательном. Между станциями данные передаются по последовательным каналам, а внутри станций обрабатываются параллельно.

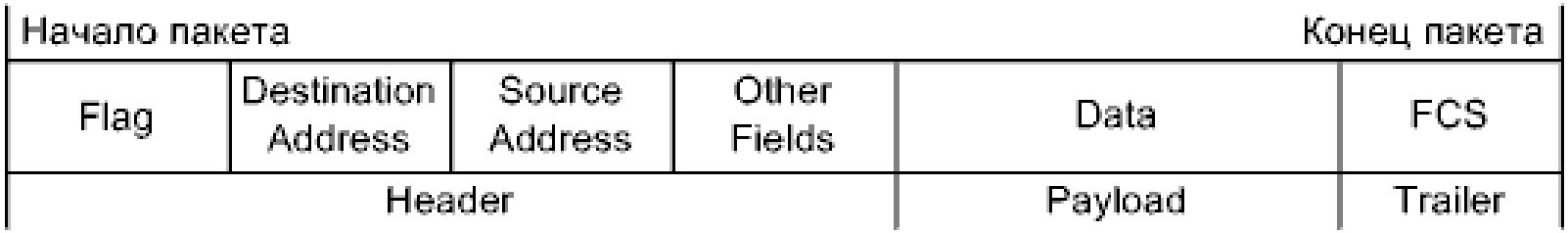
3.0.1.2

Для именования порции информации, передаваемой по каналам компьютерных (и не только компьютерных) сетей, используют обобщенный термин *пакет* (packet).

Пакет содержит последовательно сформированные станцией-передатчиком *поля* (fields), предназначенные для их интерпретации в станции-приемнике.

В общем случае, пакеты могут быть самыми разнообразными (как по структуре, так и по длине), но подавляющее большинство пакетов подпадают под типовую структуру.

3.0.1.3



Назначение полей:

Flag -- флаг, точнее, флаг начала пакета -- позволяет определить начало пакета.

Destination Address -- адрес назначения -- позволяет указать станцию, для которой предназначен пакет.

Source Address -- адрес источника -- позволяет указать станцию, сгенерировавшую пакет.

Other Fields -- прочие поля -- специфические поля (в том числе и специфические флаги) определенной реализации.

Data -- данные -- «полезное» наполнение пакета.

FCS (Frame Check Sequence) -- контрольная сумма -- позволяет проверить целостность пакета.

Структура типового пакета КС

3.0.1.4

Часть пакета, включающую поля, расположенные до начала данных, принято называть *заголовком* (header) пакета, после данных -- *хвостовиком* (trailer).

3.0.1.5

Обычно в байт-ориентированных реализациях длина пакета кратна восьми битам, то есть пакет состоит из так называемых *октетов* (octets).

При изображении структуры пакетов старшие разряды принято располагать слева или сверху (most significant bit first, big endian).

В процессе передачи, поля сдвигаются в канал по очереди, то есть начиная с левого поля.

Если поле состоит из нескольких октетов, то октеты как правило так же сдвигаются начиная с левого октета.

А вот биты октетов в реализациях сдвигаются по-разному -- как начиная с левого бита (основной вариант в семействе протоколов TCP/IP), так и начиная с правого бита (основной вариант в Ethernet); даже может быть, что биты октетов разных полей сдвигаются по-разному.

3.0.1.6

Все поля в составе любого пакета можно условно разделить на полезные и служебные.

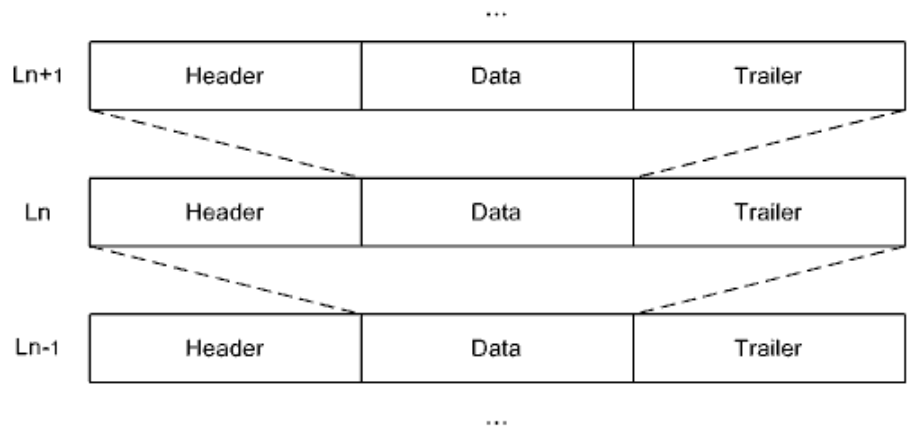
Полезная нагрузка (payload) заключается в собственно данных. Но следует понимать, что вкладываемая в качестве данных информация может носить служебный характер. В некоторых пакетах поле данных не предусмотрено вообще.

Сколько дополнительного трафика порождается в связи с наличием служебных полей оценивают как overhead.

3.0.2.1

В соответствии с концепцией модели OSI, соседние уровни абстрагированы друг от друга. Поэтому вполне закономерно, что на каждом уровне работают со своими структурами данных. При продвижении информации между уровнями возникает необходимость в преобразованиях структур данных. Преобразования выражаются в инкапсуляции и декапсуляции.

Под *инкапсуляцией* (encapsulation) в КС понимают вкладывание пакета определенного вышестоящего уровня в поле данных пакета смежного нижестоящего уровня в процессе подготовки к передаче, то есть при продвижении сверху вниз. Под *декапсуляцией* (decapsulation) понимают обратное действие после приема, то есть при продвижении снизу вверх.



3.0.2.2

Приведите пример инкапсуляции.

3.0.2.3

Как происходит декапсуляция?

3.0.2.4

Функционал любого из вышестоящих уровней «знает», какие нижестоящие ресурсы ему необходимы и чем он «располагает». Поэтому процесс инкапсуляции не доставляет трудностей.

А вот функционал нижестоящего уровня при разборе полученных пакетов заранее не знает, какой из вышестоящих подсистем передавать эти пакеты.

Проблему решают введением в структуру пакета служебного поля, в котором записывается код протокола вышестоящего уровня.

3.0.2.5

Ethertype (decimal)	Ethertype (hex)	Description
0000	0000-05DC	IEEE802.3 Length Field
0257	0101-01FF	Experimental
0512	0200	XEROX PUP (see 0A00)
0513	0201	PUP Addr Trans (see 0A01)
	0400	Nixdorf
1536	0600	XEROX NS IDP
	0660	DLOG
	0661	DLOG
2048	0800	Internet Protocol version 4 (IPv4)
2049	0801	X.75 Internet
2050	0802	NBS Internet]
2051	0803	ECMA Internet
2052	0804	Chaosnet
2053	0805	X.25 Level 3
2054	0806	Address Resolution Protocol (ARP)
2055	0807	XNS Compatability
2056	0808	Frame Relay ARP
2076	081C	Symbolics Private
2184	0888-088A	Xyplex
2304	0900	Ungermann-Bass net debugr
2560	0A00	Xerox IEEE802.3 PUP
2561	0A01	PUP Addr Trans
2989	0BAD	Banyan VINES
2990	0BAE	VINES Loopback
2991	0BAF	VINES Echo
4096	1000	Berkeley Trailer nego
4097	1001-100F	Berkeley Trailer encap/IP
5632	1600	Valid Systems
	22F3	TRILL
	22F4	L2-IS-IS
...		
	86DD	Internet Protocol version 6
...		
65535	FFFF	Reserved

3.0.2.6

Как вы думаете, что такое туннелирование (tunneling)?

3.0.2.7

Важной особенностью инкапсуляции является то, что в большинство реализаций заложена возможность передавать пакеты, относящиеся к некоторому протоколу некоторого уровня (например, сетевого), вкладывая их в пакеты другого протокола того же уровня, то есть организовывать *туннелирование* (tunneling).

3.0.2.8

Для чего может применяться туннелирование?

3.0.2.9

Инкапсуляция имеет еще ряд проявлений.

Если при выполнении инкапсуляции данные некоторого уровня не помещаются в поле отведенной длины, то можно прибегнуть к *фрагментации* (fragmentation) -- разбить данные на фрагменты и передать цепочку пакетов. Принимающая сторона будет вынуждена выполнить *дефрагментацию* (defragmentation).

Поле, отвечающее за длину поля данных, может быть не предусмотрено. Если длина поля данных фиксирована, а данных не хватает, то возникает необходимость в автодополнении (например, нулями).

3.0.2.10

Перемежение (interleaving) позволяет «распараллелить» пересылку пакетов или их фрагментов и заключается в одновременном задействовании нескольких каналов.

Особенно это применимо в низкоскоростных СрПД.

3.0.2.11

Фрагментация (при наличии альтернативных путей в СПД) и перемежение могут привести к «перемешиванию» пакетов и, как следствие, разрушению сообщения.

Контроль за порядком фрагментов может быть возложен как на протокол подверженного фрагментации уровня, так и на протокол вышестоящего уровня.

3.0.3.1

Несмотря на целостность уровней, вышестоящие уровни зависят от нижестоящих. Но степень зависимости различается.

Иногда требуется просто наличие поддержки одного из нижестоящих протоколов, иногда требуется поддержка конкретного нижестоящего протокола.

3.0.3.2

Названия структурных единиц передаваемой информации в привязке к уровням модели OSI:

L1 -- сигналы (signals).

L2 -- *кадры* (frames).

L3 -- собственно *пакеты* (packets).

L4 + L5 -- *сегменты* (segments).

L6 + L7 -- *сообщения* (messages).

Фундаментальная задача СПД заключается в том, чтобы правильно передать сообщение.

Пакеты «возникают» начиная со второго уровня, хотя собственно пакетами традиционно называют пакеты, относящиеся к третьему уровню.

Первый и второй уровни часто совмещают в рамках аппаратных технологий.

Четвертый и пятый уровни, равно как шестой и седьмой уровни, обычно реализуют «неразрывно» в рамках программных технологий.

Для обобщенной ссылки на порцию данных, над которой оперируют на некотором уровне, Cisco использует термин PDU (Protocol Data Unit).

3.0.4.1

Понятно, что для правильной интерпретации пакета нужно его считать из канала полностью, причем с соблюдением последовательности. Если бы взаимодействующие станции работали бесконечно и находились в соответствующей степени готовности, то это не составляло бы особого труда. Но, поскольку станция-приемник может подключиться к каналу (да и вообще начать работать) в произвольный момент времени, возникает проблема, связанная с распознаванием флага начала пакета.

Флаг начала пакета представляет собой зарезервированную цифровую последовательность, которая собственно позволяет станции-приемнику определить начало пакета.

Проблема заключается в том, что такая же последовательность вполне может встретиться в пакете и после флага начала. Следовательно, возникает задача обеспечения уникальности флага начала пакета, то есть исключения этой последовательности из оставшейся части пакета.

Это достигается за счет действия, заключающегося в модификации следующей за флагом цифровой последовательности, которое в бит-ориентированных системах называют *бит-стаффингом* (bit stuffing), а в байт-ориентированных -- *байт-стаффингом* (byte stuffing).

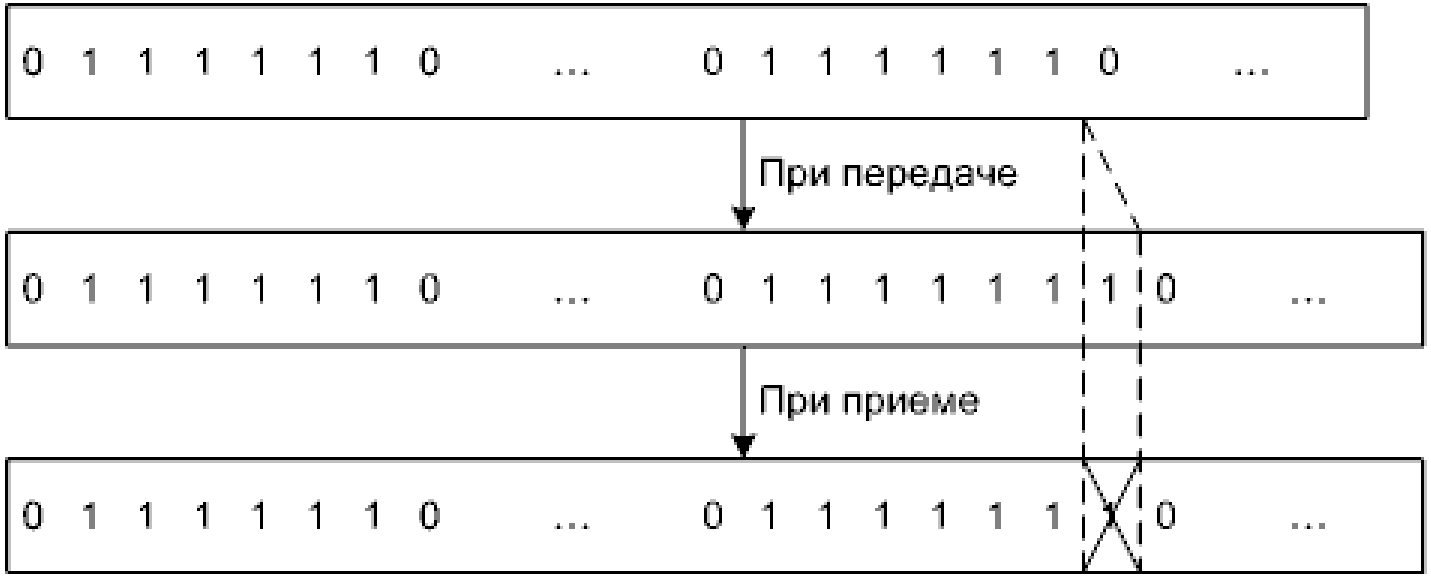
3.0.4.2

При бит-стаффинге совпадающая с флагом последовательность разбивается с помощью вставки дополнительно бита с соответствующим значением.

Применение бит-стаффинга приводит к увеличению длины пакета. Теоретически, с целью уменьшения связанных с бит-стаффингом «издержек», следует стремиться к минимизации количества вставок: разбивающий бит нужно вставлять после наиболее длинной уникальной подпоследовательности в флаговой последовательности.

3.0.4.3

Классическим флагом начала пакета является байт со значением 01111110b (7Eh).



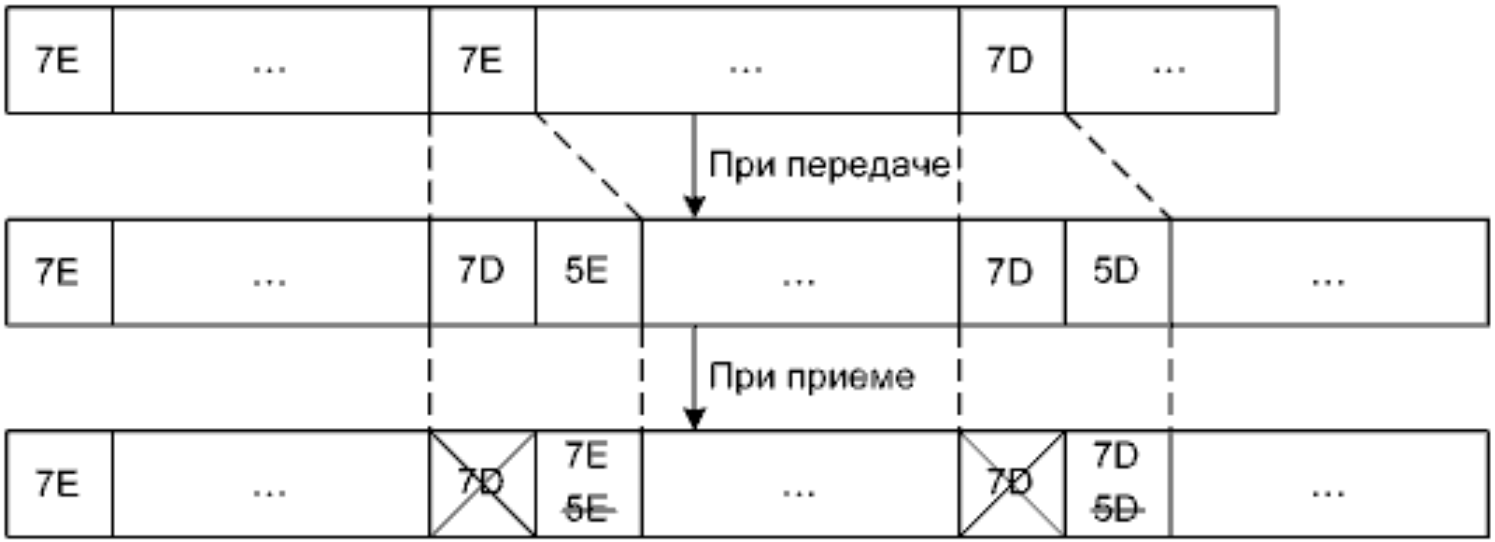
На передающей стороне после нуля и шести единиц всегда вставляется седьмая единица, а на принимающей стороне единица после нуля и шести единиц всегда удаляется.

3.0.4.4

Цель байт-стаффинга полностью совпадает с целью бит-стаффинга.

В сравнении с алгоритмами бит-стаффинга, алгоритмы байт-стаффинга манипулируют байтами, являются более сложными и более «затратными», но при программировании они позволяют избежать битовых операций (бит-стаффинг, в отличие от байт-стаффинга, обычно реализуют аппаратно).

3.0.4.5



Единственным способом обеспечения уникальности флагового байта является замена совпадающего с ним байта на некий выбранный другой. Но возникает вопрос, как принимающая сторона отличит замененный байт от такого же незамененного. Решением является применение так называемого ESC-символа. Наличие ESC-символа говорит станции-приемнику о факте замены, а следующий за ESC-символом символ -- код замены позволяет определить какая замена была осуществлена. Байт-стаффингу можно подвергать целые группы символов.

3.0.4.6

Бит-стаффинг обычно применяют при задействовании синхронных СрПД, а байт-стаффинг -- асинхронных.

Примерами технологий могут служить SDLC, HDLC, ISDN и другие (многие поддерживают как синхронные так и асинхронные СрПД).

Примером протокола может служить PPP.

Следует отметить, что на практике (например, применительно к HDLC) бит-стаффинг выполняется вставкой нуля после пяти единиц.

3.0.4.7

Нарисуйте принципиальную схему устройства, которое будет выполнять бит-стаффинг и де-бит-стаффинг применительно к стандартному флагу.