

Протокол межсетевых управляющих сообщений ICMP

Для того, чтобы маршрутизаторы могли оповещать узлы сети о возникших ошибках или нештатных ситуациях, в стек TCP/IP введен механизм рассылки специальных сообщений, который назвали протоколом межсетевых управляющих сообщений (Internet Control Message Protocol, или ICMP).

Протокол ICMP - это протокол уведомления об ошибках, а не коррекции ошибок. Маршрутизатор или узел сети может предпринять некоторые действия для того, чтобы ошибка больше не возникала, но эти действия протоколом ICMP не регламентируются.

Доставка сообщений протокола ICMP

Протокол ICMP позволяет маршрутизаторам отправлять другим маршрутизаторам или узлам сети сообщения об ошибках или управляющие сообщения. Протокол ICMP обеспечивает средство связи между программами протокола IP двух компьютеров.

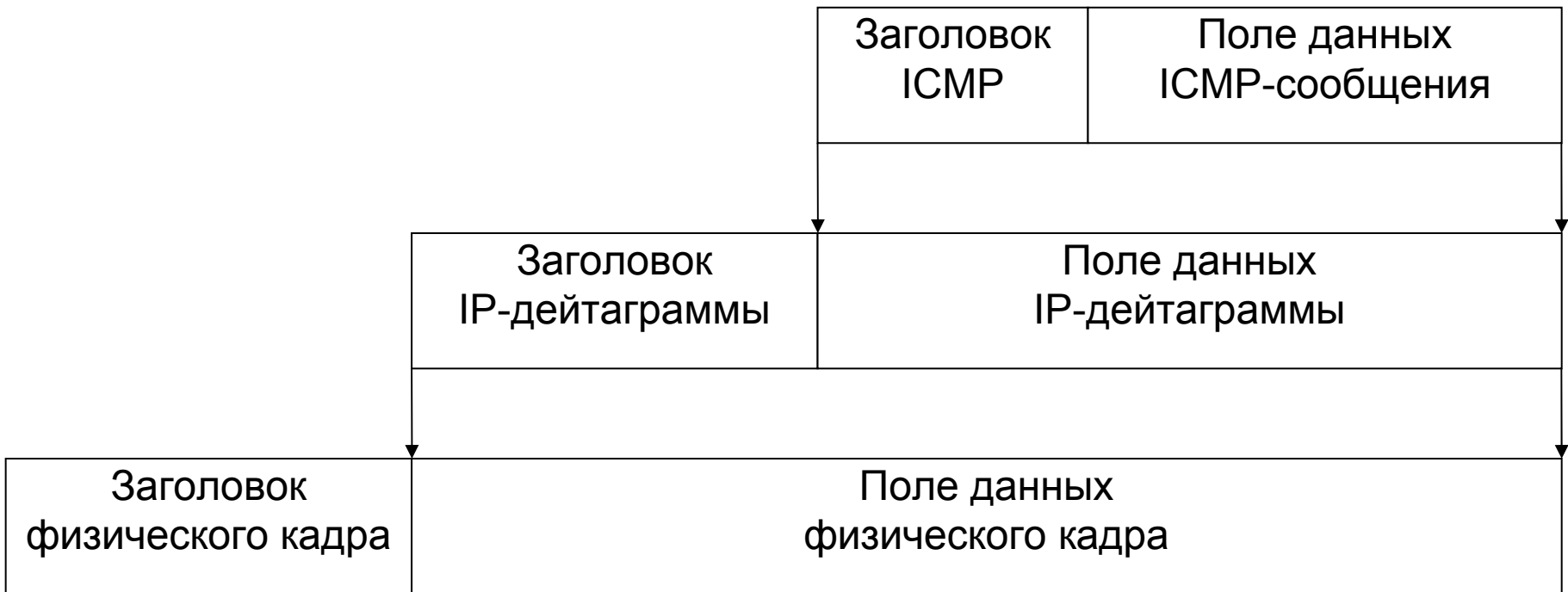


Рис. Инкапсуляция ICMP-сообщения в IP-дейтаграмму, которая затем помещается в поле данных физического кадра. Для идентификации ICMP-сообщения в поле типа протокола заголовка IP-дейтаграммы помещается значение 1

Формат сообщений протокола ICMP

Существует несколько типов сообщений ICMP, каждый из которых имеет свой формат, но при этом все они начинаются с общих трех полей:

- 8-битного целого поля, обозначающего тип сообщения (type), идентифицирующего сообщение;
- 8-битного поля кода (code), значение которого конкретизирует назначение сообщения,
- 16-битного поля контрольной суммы (checksum).

Формат сообщений протокола ICMP

Значения полей		Описание ICMP-сообщения
Тип	Код	
0		Ответ на запрос эха
3		Получатель недоступен
	0	Сеть недоступима
	1	Узел сети недоступим
	2	Протокол недоступен
	3	Порт недоступен
	4	Необходима фрагментация, однако установлен бит ее запрета
	5	Ошибка маршрутизации от источника
	6	Сеть получателя неизвестна
	7	Узел получателя неизвестен
	8	Узел отправителя изолирован
	9	Связь с сетью получателя запрещена администратором
	10	Связь с узлом получателя запрещена администратором
	11	Сеть недоступима для данного типа обслуживания
12	Узел недоступим для данного типа обслуживания	

Формат сообщений протокола ICMP

Значения полей		Описание ICMP-сообщения
Тип	Код	
4		Подавление источника данных
5		Переадресация (изменения маршрута)
	0	Переадресовать дейтаграммы для указанной сети (устарело)
	1	Переадресовать дейтаграммы для указанного узла сети
	2	Переадресовать дейтаграммы с указанным типом обслуживания и для указанной сети
	3	Переадресовать дейтаграммы с указанным типом обслуживания и для указанного узла сети
8		Запрос эха
9		Извещение о маршрутизаторе
10		Запрос на адрес маршрутизатора
11		Истекло время ожидания фрагментов или время жизни дейтаграммы
	0	Исчерпано значение счетчика времени жизни дейтаграммы
	1	Истекло время ожидания при получении фрагментов дейтаграммы

Запрос эха и ответное сообщение

0	8	16	24	31
Тип (8 или 0)		Код (0)	Контрольная сумма	
Идентификатор			Порядковый номер	
Необязательные данные ...				

Рис. Формат запроса на эхо и ответного ICMP-сообщения

Недостижимость получателя

0	8	16	24	31
Тип (3)	Код (0-12)	Контрольная сумма		
Не используются (должны быть нули)				
Заголовок и первые 64 бита поля данных дейтаграммы				
...				

Рис. Формат ICMP-сообщения о недостижимости получателя

При невозможности переслать или доставить дейтаграмму получателю, маршрутизатор уведомляет ее отправителя, так как сам маршрутизатор не может выявить всевозможные проблемы с ее доставкой.

Подавление источника данных

0	8	16	24	31
Тип (3)	Код (0-12)	Контрольная сумма		
Не используются (должны быть нули)				
Заголовок и первые 64 бита поля данных дейтаграммы				
...				

Рис. Формат ICMP-сообщения о подавлении источника данных. В случае перегрузки маршрутизатор использует это сообщение, помещая в него первые 64 бита дейтаграммы, для уведомления отправителя о каждой утерянной дейтаграмме

Переадресация дейтаграмм

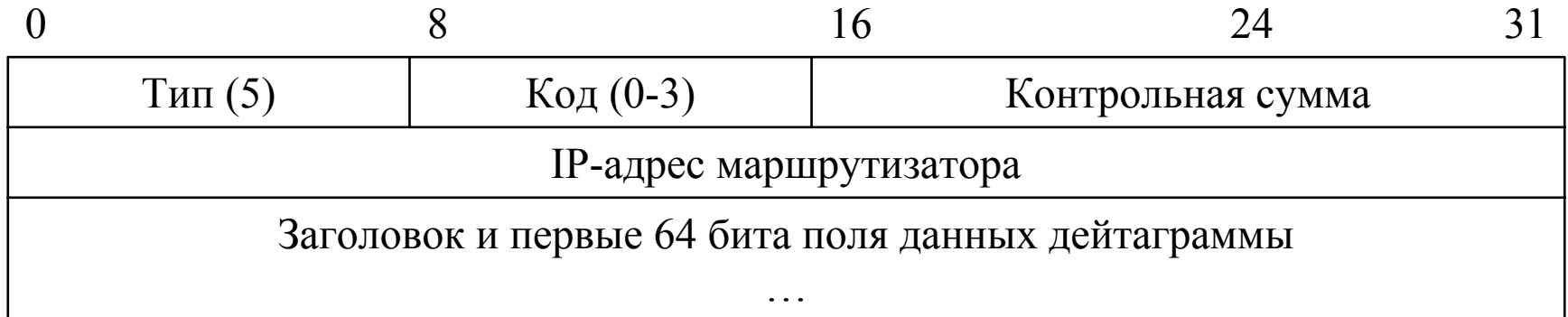


Рис. Формат ICMP-сообщения о переадресации

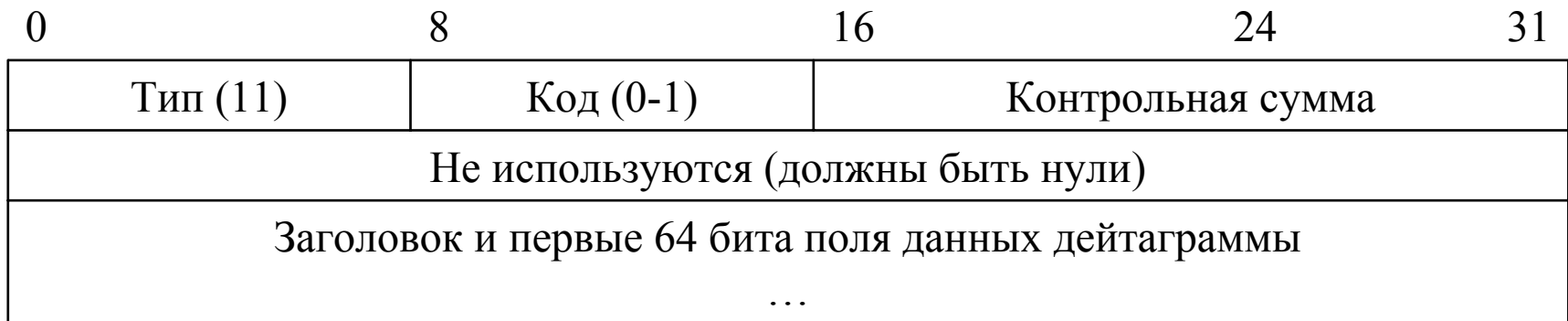
Маршрутизаторы отправляют ICMP-сообщения о переадресации только узлам сети, а не другим маршрутизаторам. Для обмена маршрутной информацией между маршрутизаторами существуют специальные протоколы.

Поиск маршрутизатора

0	8	16	24	31
Тип (9)	Код (0)	Контрольная сумма		
Количество адресов	Размер адреса (1)	Время жизни		
Адрес маршрутизатора 1				
Приоритет маршрутизатора 1				
Адрес маршрутизатора 2				
Приоритет маршрутизатора 2				
...				

Рис. Формат ICMP-сообщения, используемый для извещения узлов сети об адресах маршрутизаторов. Такие сообщения периодически рассылаются самими маршрутизаторами

Истечение времени ожидания



*Рис. Формат ICMP-сообщения об истечении времени ожидания.
Маршрутизатор посылает такое сообщение отправителю дейтаграммы тогда, когда значение поля время жизни дейтаграммы стало меньше нуля или закончилось время ожидания при получении фрагментов дейтаграммы*

Ошибка в параметрах дейтаграммы

0	8	16	24	31
Тип (12)	Код (0-1)	Контрольная сумма		
Указатель	Не используются (должны быть нули)			
Заголовок и первые 64 бита поля данных дейтаграммы				
...				

*Рис. Формат ICMP-сообщения об ошибке в параметрах дейтаграммы.
Подобное сообщение посылается отправителю только в случае
удаления дейтаграммы из сети*

Оценка времени передачи

0	8	16	24	31
Тип (13 или 14)	Код (0)	Контрольная сумма		
Идентификатор		Порядковый номер		
Время отправления запроса				
Время получения запроса				
Время отправления ответа				

*Рис. Формат ICMP-сообщения
запрашивающего временную метку и ответ*

Определение маски подсети

0	8	16	24	31
Тип (17 или 18)	Код (0)	Контрольная сумма		
Идентификатор		Порядковый номер		
Маска адреса подсети				

Рис. Формат ICMP-запроса маски подсети и ответного сообщения. Обычно запрос на маску подсети посылается в широковещательном режиме, так как адрес маршрутизатора еще не известен

ICMP : основные выводы

В протоколе межсетевых управляющих сообщений (ICMP) предусмотрены специальные средства взаимодействия между маршрутизаторами и узлами сети. Этот протокол является неотъемлемой и обязательной частью протокола IP, и осуществляет:

- передачу отклика на пакет или эхо на отклик;
- контроль времени жизни дейтаграмм в системе;
- реализует переадресацию пакета;
- выдает сообщения о недостижимости адресата или о некорректности параметров;
- формирует и пересылает временные метки;
- выдает запросы и отклики для адресных масок и другой информации.

Перед отправкой ICMP-сообщение помещается в поле данных IP-дейтаграммы. Заголовок ICMP-сообщения начинается с трех стандартных полей фиксированной длины: тип сообщения, код сообщения и контрольная сумма. Значение поля типа определяет формат остальной части сообщения и его назначение. ICMP-сообщения об ошибках никогда не выдаются в ответ на:

- ICMP-сообщение об ошибке.
- При многоадресной или широковещательной адресации.
- Для фрагмента дейтограммы (кроме первого).
- Для дейтаграмм, адрес отправителя которых является нулевым, широковещательным или многоадресным.

Протокол передачи пользовательских дейтаграмм UDP

Номер порта, задаваемый транспортным уровнем, в совокупности с номером сети и номером компьютера, задаваемые сетевым уровнем, однозначно определяют прикладной процесс в сети.

Протокол передачи пользовательских дейтаграмм (User Datagram Protocol или UDP) является протоколом транспортного уровня, и обеспечивает ненадежную доставку сообщений без установления логического соединения заданным программам на конкретном компьютере, адресуясь к ним по номеру порта протокола.

Программы протокола IP отвечают только за передачу данных между компьютерами объединенной сети. Программы протокола UDP выполняют разделение потоков данных между различными источниками или получателями одного компьютера.

Транспортный
уровень

Заголовок
UDP

Поле данных
UDP-дейтаграммы

Сетевой
уровень

Заголовок
IP-дейтаграммы

Поле данных
IP-дейтаграммы

Заголовок
физического кадра

Поле данных
физического кадра

Рис. Инкапсуляция UDP-дейтаграммы в IP-дейтаграмму, которая каждый раз перед передачей по заданному участку физической сети инкапсулируется в физический кадр

Формат UDP-дейтаграммы

0	8	16	24	31
Номер порта отправителя		Номер порта получателя		
Длина UDP-дейтаграммы		Контрольная сумма		
Область данных ...				

Рис. Формат пользовательской дейтаграммы

0	8	16	24	31
IP-адрес отправителя				
IP-адрес получателя				
Нули	Тип UDP (17)		Длина UDP-дейтаграммы	

Рис. Формат псевдозаголовка размером 12 байт, который используется для вычисления контрольной суммы UDP-дейтаграммы

Мультиплексирование и демультимплексирование UDP-дейтаграмм

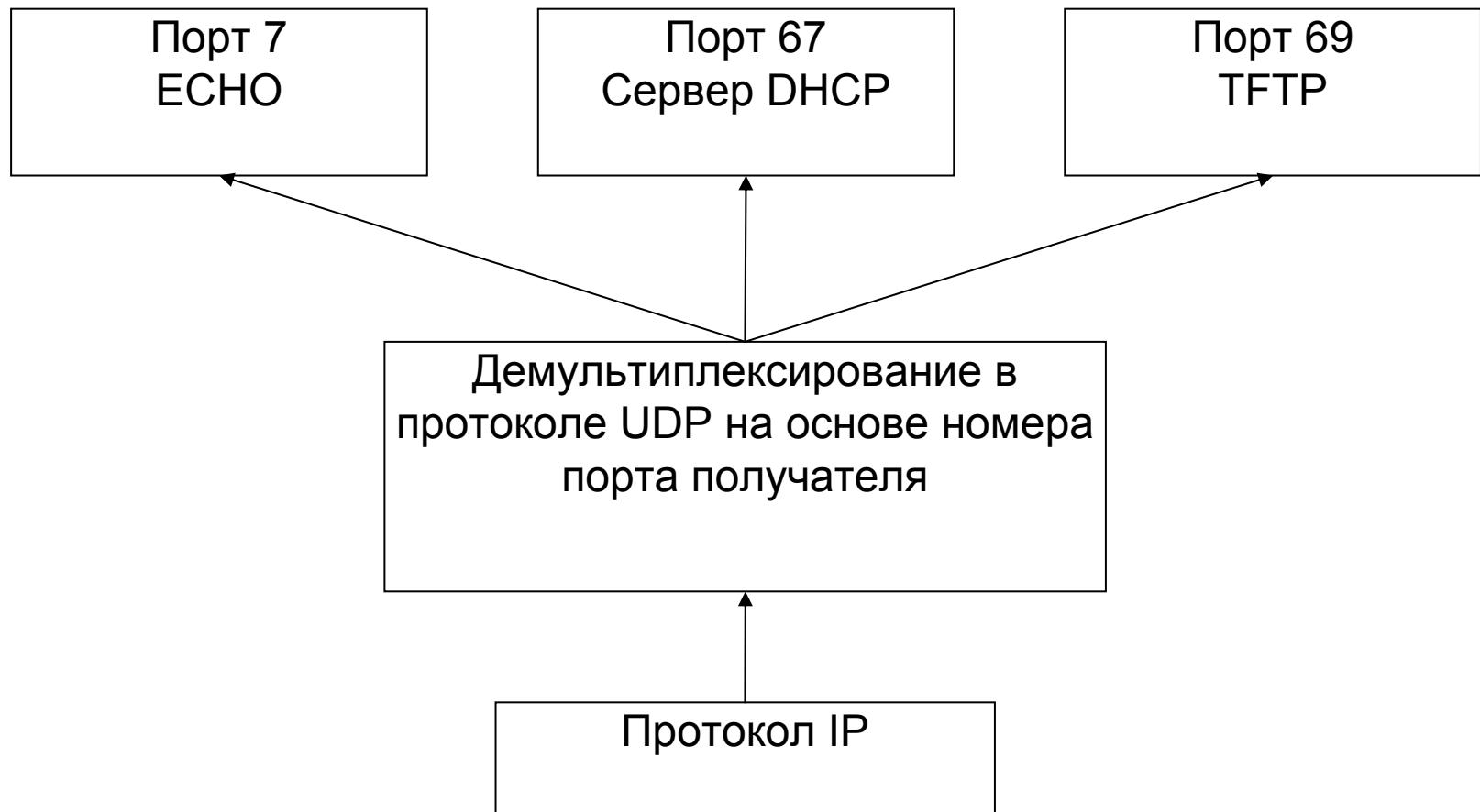


Рис. Пример демультимплексирования в протоколе UDP. При выборе соответствующего номера порта для поступивших дейтаграмм в программе протокола UDP используется поле номера порта получателя заголовка UDP-дейтаграммы

UDP : основные выводы

На языке многозадачных операционных систем выполняющиеся в них программы называются процессами. В протоколе передачи пользовательских дейтаграмм (User Datagram Protocol, или UDP) предусмотрен механизм, позволяющий распознавать поступающие пользовательские дейтаграммы и передавать их на обработку одному из процессов компьютера конечного получателя. Для этого в заголовке UDP-дейтаграммы предусмотрены два 16-битовых целых числа, называемые номерами портов отправителя и получателя. Часть широко известных номеров портов зарезервирована и используется стандартными службами глобальной сети Интернет. Остальные номера портов могут свободно использоваться в прикладных программах. Также в формат заголовка UDP-дейтаграммы входит еще два поля: длина всей дейтаграммы и контрольная сумма.

Единственное назначение протокола UDP это предоставление прикладным программам простого, ненадежного и не требующего соединения транспортного средства с протоколом IP. Поэтому UDP-сообщения могут быть потеряны, продублированы, задержаны или доставлены в произвольном порядке, и эти проблемы должны решаться самостоятельно прикладными программами.

Надежная потоковая транспортная служба TCP

Есть несколько особенностей, которые характеризуют интерфейс между прикладными программами и надежной службой доставки пакетов:

- Установление логического соединения
- Использование потоков данных
- Дуплексное соединение
- Использование буферов
- Неструктурированные потоки

В качестве основной абстракции в протоколе TCP используется понятие логического соединения, а не номера порта. Логическое соединение идентифицируется с помощью пары конечных точек: IP-адреса и номера TCP-порта. Поскольку соединение устанавливается между двумя конечными точками, то один номер TCP-порта может использоваться в нескольких логических соединениях, открытыми на одном и том же компьютере.

Установление TCP-соединений

TCP обеспечивает надежную транспортировку данных между прикладными процессами различных компьютеров путем установления между ними логического соединения.

Установление логического соединения выполняется в следующей последовательности:

- При установлении соединения сторона инициатор, посылает запрос к протоколу TCP на открытие порта для передачи (*active open*).
- После открытия порта протокол TCP на стороне процесса-инициатора посылает запрос процессу, с которым требуется установить соединение.
- Протокол TCP на приемной стороне открывает порт для приема данных (*passive open*) и возвращает подтверждение о приеме запроса.
- Для того чтобы передача могла вестись в обе стороны, протокол на приемной стороне также открывает порт для передачи (*active port*) и также передает запрос к противоположной стороне.
- Сторона-инициатор открывает порт для приема и подтверждает прием. Соединение считается установленным.

Сегменты и потоки TCP

В протоколе TCP перед передачей по сети, поток неструктурированных данных поступающий от прикладных программ, разбивается на сегменты. Сегмент – это последовательность пронумерованных байт. Как правило, каждый сегмент данных передается по сети в виде одной IP-дейтаграммы.

Концепция квитирования

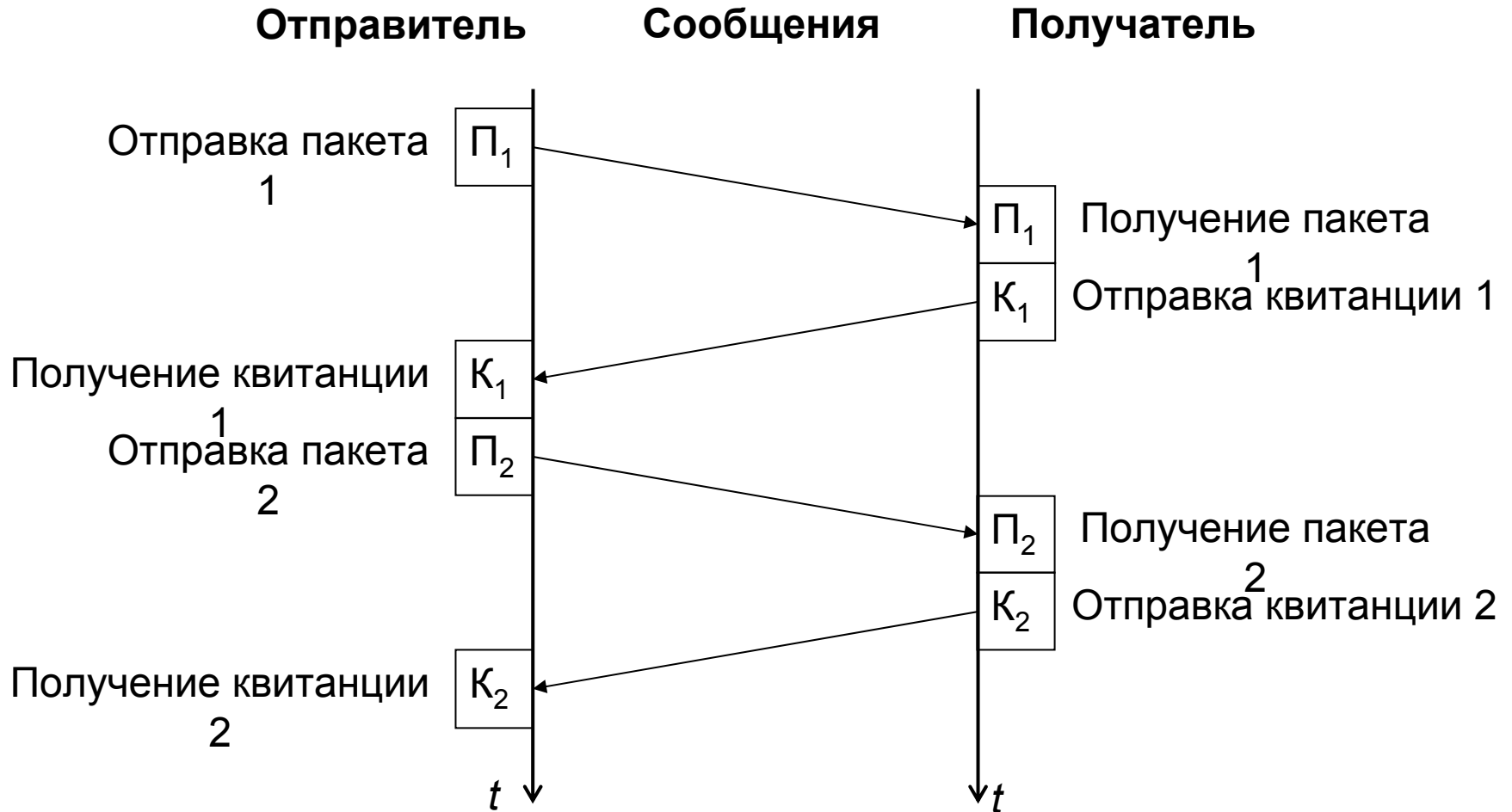
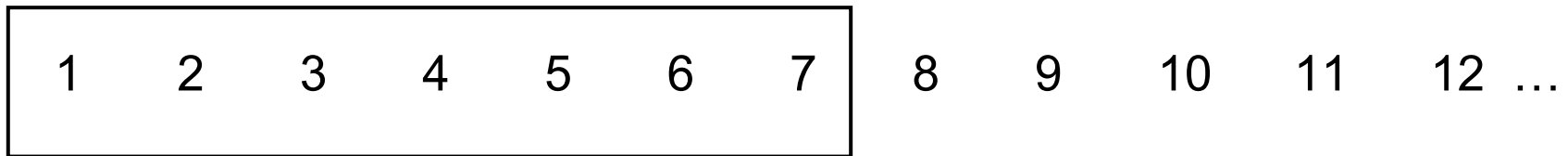


Рис. Механизм подтверждения приема с повторной передачей, при которой отправитель простаивает, ожидая уведомления об успешном получении каждого пакета

Реализация скользящего окна в протоколе TCP

Начальное положение окна



(а)

Сдвиг окна →



(б)

Рис. Окно, внутрь которого помещено 7 пакетов (а); при получении подтверждения о приеме пакета 1 окно сдвигается на один пакет в право, и в сеть отправляется 8-й пакет (б). Если для какого-либо пакета, попавшего в окно не получена квитанция, то выполняется повторная передача этого пакета

Реализация скользящего окна в протоколе TCP



Рис. Пример скользящего окна протокола TCP. Байты 1-3 были отправлены и на них пришли положительные квитанции; байты 4-7 отправлены в сеть, но подтверждения об их успешной доставке еще не получено; байты 8-10 могут быть отправлены в сеть без всяких задержек; остальные байты с 11 и выше не могут быть отправлены в сеть до тех пор, пока не попадут внутрь окна

В квитанциях подтверждения приема протокола TCP указывается порядковый номер следующего байта в потоке, который ожидает получатель.

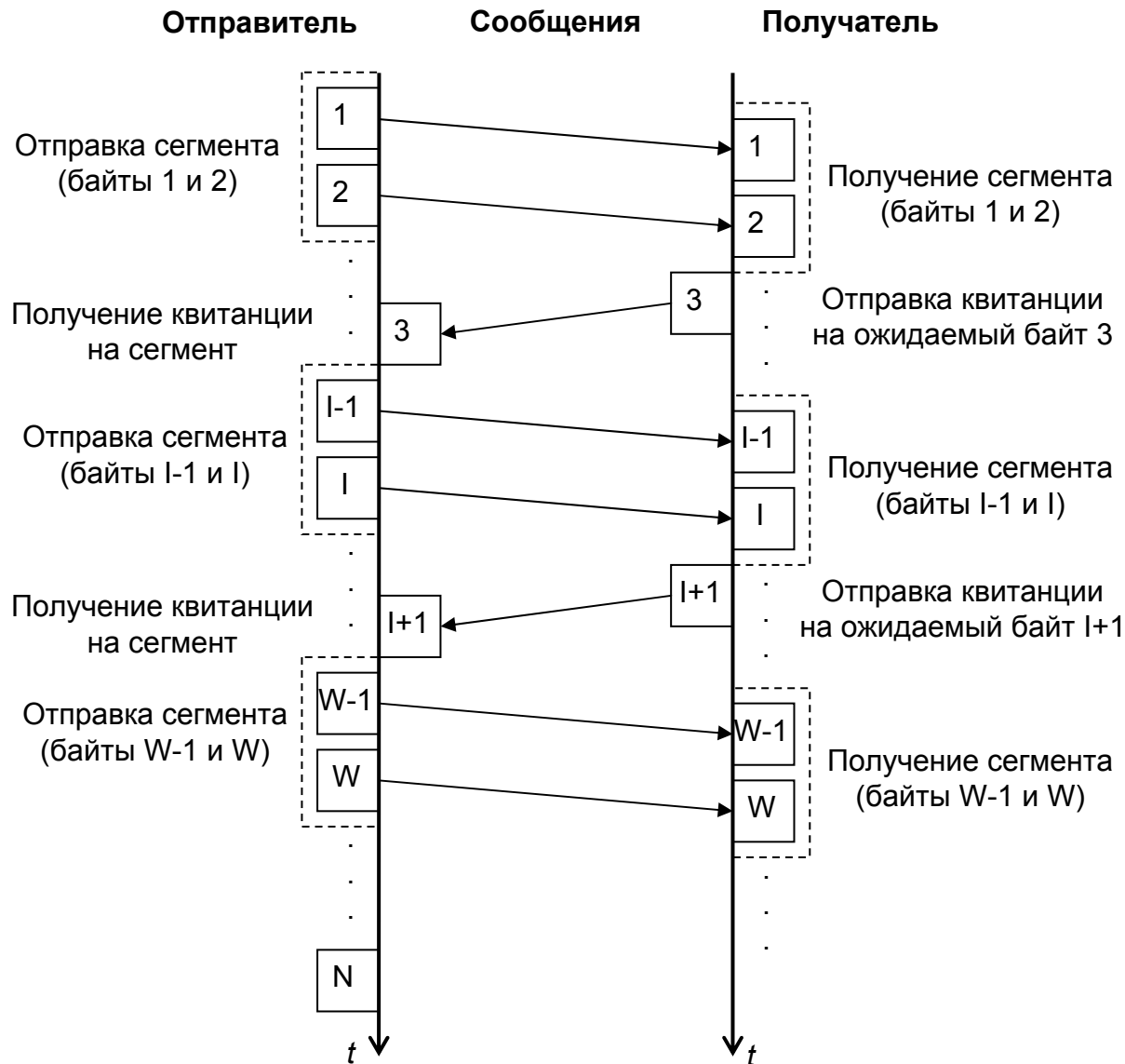


Рис. Метод скользящего окна. Идея заключается в том, что источник может отправить в сеть сразу все пакеты с номерами входящими в текущее окно размером W , не дожидаясь квитанций о подтверждении их приема

Выбор тайм-аута и повторная передача сегментов

Для учета большего разброса задержек по времени доставки пакетов в реальной объединенной сети, в протоколе TCP используется адаптивный алгоритм повторной передачи. Значение тайм-аута выбирается в соответствии с текущим временем задержки доставки пакета, которое постоянно отслеживается для всех открытых соединений.

Алгоритм Карна при вычислении предполагаемого полного времени доставки пакета (времени оборота) не учитывает замеры для повторно отправленных сегментов, а использует методику увеличения значения тайм-аута.

Управление размером окна и перегрузкой

При использовании метода скользящего окна правильный выбор размера окна позволяет полностью исключить простои в сети и достичь большей эффективности потоковой передачи данных по сравнению с методом подтверждения приема с повторной передачей.

Каждый раз после возникновения перегрузки в сети размер окна уменьшается в два раза (вплоть до одной дейтаграммы), что определяется стратегией мультипликативного уменьшения. Для сегментов попавших в окно нового размера, применяется стратегия экспоненциального увеличения значения таймера повторной передачи (тайм-аута).

Управление размером окна и перегрузкой

Методика медленного старта предназначена для восстановления работоспособности сети после перегрузки, а также для начала передачи данных по новому соединению. При этом первоначальный размер окна перегрузки выбирается равным одному сегменту и каждый раз после получения квитанции подтверждения приема он увеличивается на один сегмент.

Для раннего обнаружения и устранения перегрузки в маршрутизаторах, используется алгоритм RED. Если входная очередь дейтаграмм переполнена, то все вновь поступающие дейтаграммы аннулируются. Если же входная очередь не заполнена до конца, но ее размер превышает заранее установленный минимальный порог, то во избежание эффекта глобальной синхронизации, одна из поступивших дейтаграмм, выбранная случайным образом в соответствии с рассчитанной долей вероятности, удаляется.

Формат сообщений TCP

0	4	8	16	24	31
Номер порта отправителя			Номер порта получателя		
Порядковый номер					
Номер подтверждения					
Длина заг.	Резерв	Код сегмента	Размер окна		
Контрольная сумма			Указатель срочных данных		
Опции протокола TCP (если есть)				Выравнивание	
Область данных					
...					
...					

Рис. Формат TCP-сегмента, состоящего из заголовка и области данных. Сегменты используются не только для передачи данных, но также в качестве квитанции подтверждающей прием, установки и разрыва логического соединения

Формат сообщений TCP

Название бита	Значение
URG	В заголовке присутствует указатель срочных данных
ACK	В заголовке указано поле подтверждения приема
PSH	В данном сегменте указан запрос на немедленную отправку данных
RST	Сброс соединения
SYN	Сообщение используемое для синхронизации счетчиков переданных данных при установлении соединения
FIN	Признак достижения передающей стороной последнего байта в потоке передаваемых данных

Рис. Значения битов кода сегмента TCP-заголовка

Управление логическим соединением

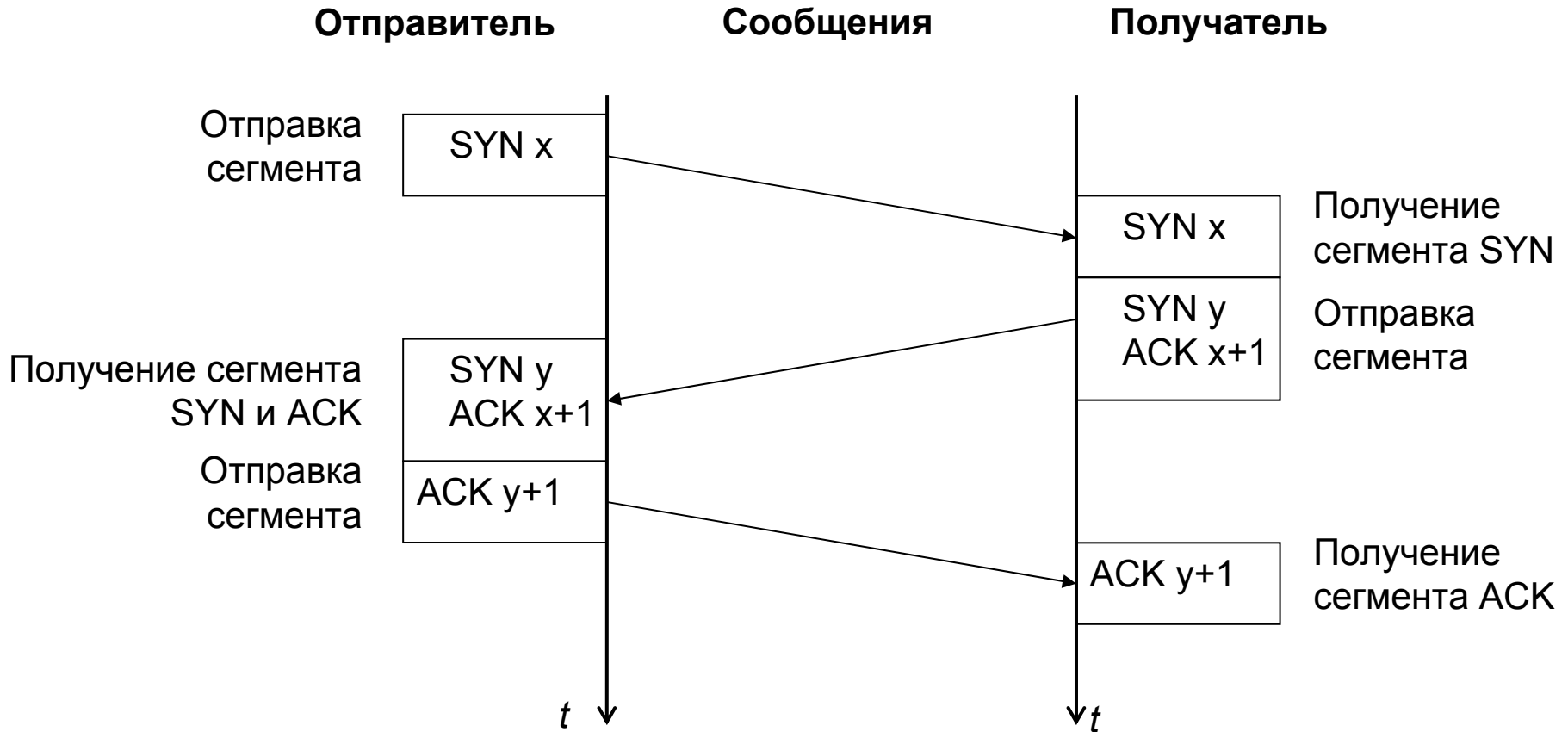


Рис. Последовательность сообщений, посылаемых при установлении соединения во время трехэтапного метода квитирования. В сегменте типа SYN пересылается начальный порядковый номер

Управление логическим соединением

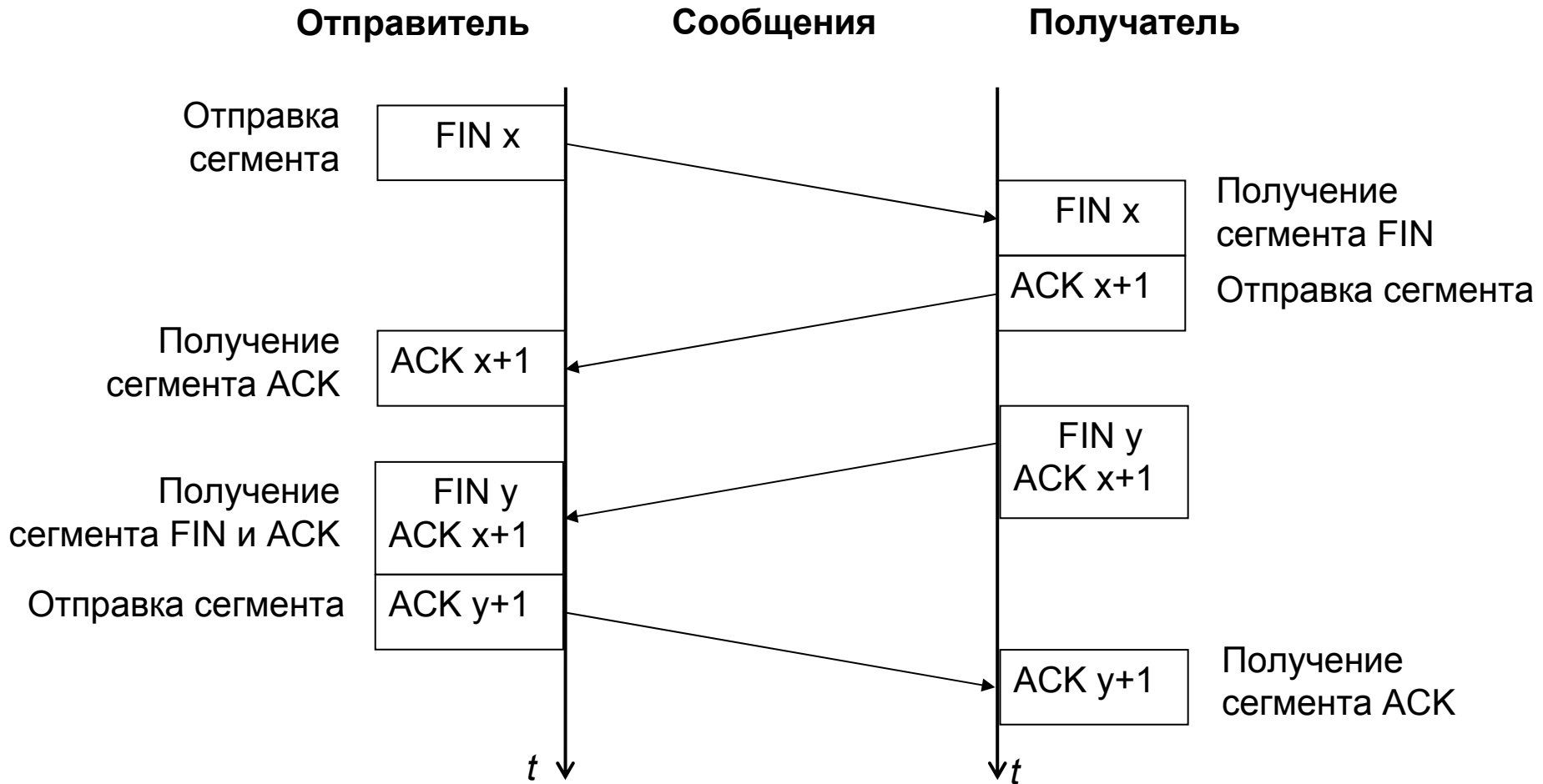


Рис. Последовательность сообщений, посылаемых при закрытии TCP-соединения. Для идентификации сегмента закрытия используется бит FIN

TCP : основные выводы

В протоколе TCP определены стандарты на одно из основных служб объединенной сети – надежную потоковую транспортную службу. Стандартом протокола TCP предусмотрена установка дуплексного режима обмена между компьютерами, что позволяет эффективно обмениваться большими объемами данных.

Для повышения эффективности передачи данных по сети в протоколе TCP предусмотрен механизм скользящих окон, который позволяет отправлять в сеть сразу некоторую последовательность данных и при этом контролировать успешность ее доставки.

Протокол TCP не зависит от низкоуровневой системы доставки данных и поэтому может быть использован практически в любых сетях. Механизм управления реализованный в протоколе TCP позволяет организовать обмен данными, между компьютерами, работающими на разных скоростях.

Основная единица передачи данных в протоколе TCP – сегмент. Сегменты используются не только для передачи данных, но также и для передачи служебной информации, необходимой для установления и разрыва соединения между двумя компьютерами.

В современной версии стандарта TCP используется метод экспоненциальной коррекции тайм-аута, позволяющей более точно определять время повторной передачи сегментов. Для предотвращения перегрузок, в протоколе TCP используются методы медленного старта и мультипликативного уменьшения.