# Управляющий протокол ICMP. Сигнализирующие сообщения

## Общие сведения

* Протокол сетевого уровня;
* Решает задачи
  + управления,
  + нотификации об ошибках,
  + тестирования и мониторинга;
* Инкапсулируется в IP *(да, протокол сетевого уровня в протоколе сетевого уровня)*;
* Описан в RFC792.

Задачи управления и нотификации – базовые функции сетевого уровня. При этом авторы архитектуры не зашили это в протокол IP, а выделили в отдельный протокол. Один из важнейших для стека TCP/IP.

ICMP-трафик обычно не пускают на широковещательные адреса.

## Организация протокола ICMP

Общая часть заголовка *(8, 8, 16 бит)*:



* Тип – тип пакета;
* Код – расшифровка типа (подтип);
* Контрольная сумма вычисляется для всего пакета.

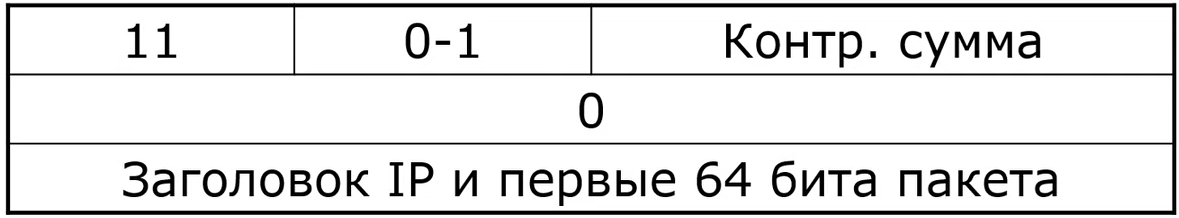
Остальная часть пакета зависит от типа ICMP-пакета.

## Нотификационные (сигнализирующие) сообщения

Информируют отправителя о каком-либо событии в сети.

*Нотификационные сообщения фильтровать нельзя!*

Основные типы:

* 3 – получатель недостижим *(нельзя фильтровать в своей сети)*:  
  
  + Тип (3);
  + Код *(причина «недостижимости»)*:
    - 0 – сеть недостижима;
    - 1 – узел недостижим;
    - 2 – протокол недостижим *(например, хотим доставить по TCP, но приемная сторона его не поддерживает)*;
    - 3 – порт недостижим *(когда никто {сервис, приложение} не прослушивает порт)*;
    - 4 – требуется фрагментация *(в IP-пакете установлен флаг, запрещающий фрагментацию, но сам пакет слишком большой для передачи целиком по каналу)*;
    - 5 – ошибка маршрутизации от источника *(когда не можем строго пройти через указанные адреса {строгая маршрутизация от источника в IP})*;
    - 6 – сеть назначения неизвестна *(обычно – попытки маршрутизации в сеть класса Е, то есть в адреса, которые не маршрутизируются в сетях TCP/IP)*;
    - 7 – узел назначения неизвестен *(cм. 6)*;
    - 8 – отправитель изолирован *(обычно – нет действующих интерфейсов для отправки пакета)*;
    - 9 – взаимодействие с сетью назначения административно запрещено *(фаервол – стоит правило REJECT {а вообще есть accept, deny, reject, но обычно во избежание перегрузки сети ответными пакетами ставят DENY и молча отбрасывают пакеты})*;
    - 10 – взаимодействие с узлом назначения административно запрещено *(см 9)*.
    - 11 – сеть недостижима из-за класса обслуживания *(используются разряды TOS, на всех маршрутизаторах внутри сети настроено управление качеством обслуживания, а мы запросили сервис выше нашего уровня)*;
    - 12 – узел недостижим из-за класса обслуживания *(см. 11)*.
  + Контрольная сумма;
  + Нулевое слово;
  + Заголовок и первые два слова пакета *(который не смогли доставить)*;
* 11 – превышено время *(нельзя фильтровать в своей сети)*:  
  
  + Тип (11);
  + Код:
    - 0 – превышено TTL;
    - 1 – превышено время ожидания фрагмента при сборке;
  + Последнее поле содержит первую часть пакета, фрагмент которого не дошел;
* 12 – ошибка параметра *(нельзя фильтровать в своей сети)*:  
  
  + Тип (12);
  + Указатель (байтовый). *(В случае, если какой-либо из промежуточных маршрутизаторов или конечный узел, проанализировав заголовок IP-пакета, определил, что произошла ошибка {невалидное значение поля, неверная контрольная сумма…}, он сообщает о ней, указывая номер ошибочного байта)*;
  + Последнее поле содержит первую часть пакета, в котором обнаружена ошибка;

# Управляющий протокол ICMP. Управляющие и тестовые сообщения

## Общие сведения

* Протокол сетевого уровня;
* Решает задачи
  + управления,
  + нотификации об ошибках,
  + тестирования и мониторинга;
* Инкапсулируется в IP *(да, протокол сетевого уровня в протоколе сетевого уровня)*;
* Описан в RFC792.

Задачи управления и нотификации – базовые функции сетевого уровня. При этом авторы архитектуры не зашили это в протокол IP, а выделили в отдельный протокол. Один из важнейших для стека TCP/IP.

ICMP-трафик обычно не пускают на широковещательные адреса.

## Организация протокола ICMP

Общая часть заголовка *(8, 8, 16 бит)*:



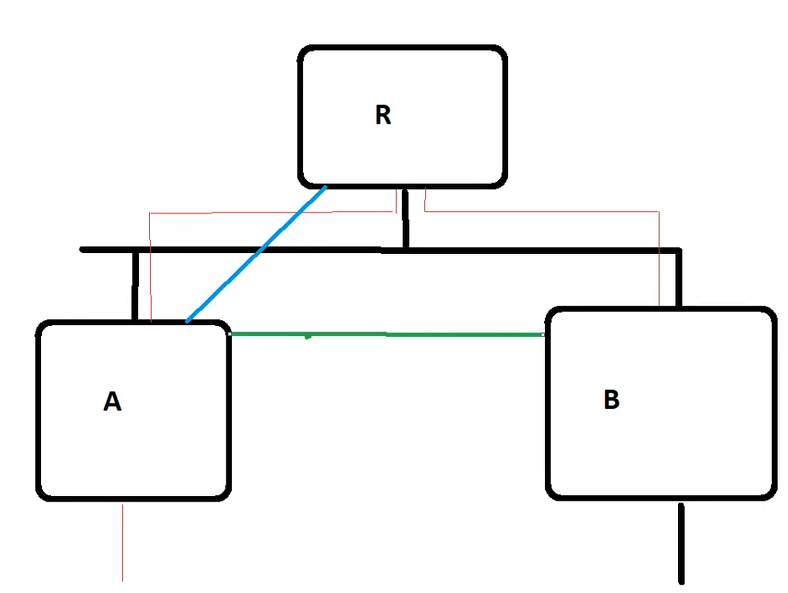
* Тип – тип пакета;
* Код – расшифровка типа (подтип);
* Контрольная сумма вычисляется для всего пакета.

Остальная часть пакета зависит от типа ICMP-пакета.

## Управляющие сообщения

Управляющие сообщения – попытка «повлиять» на саму сеть.

Основные типы:

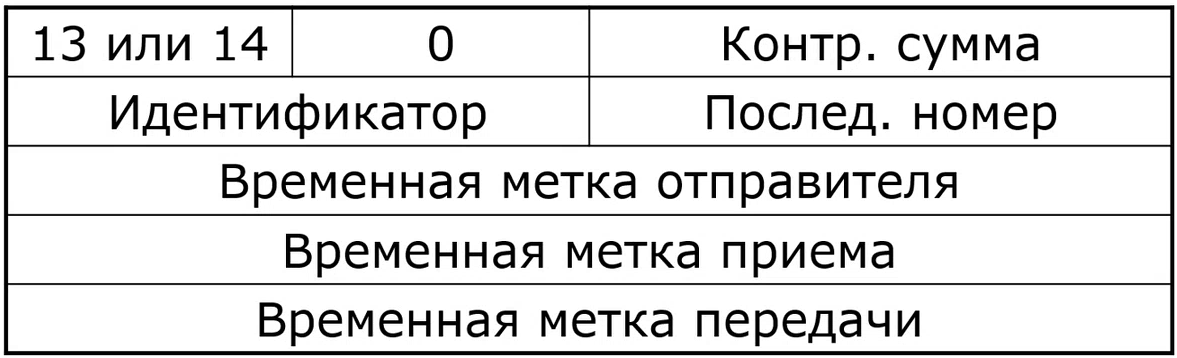
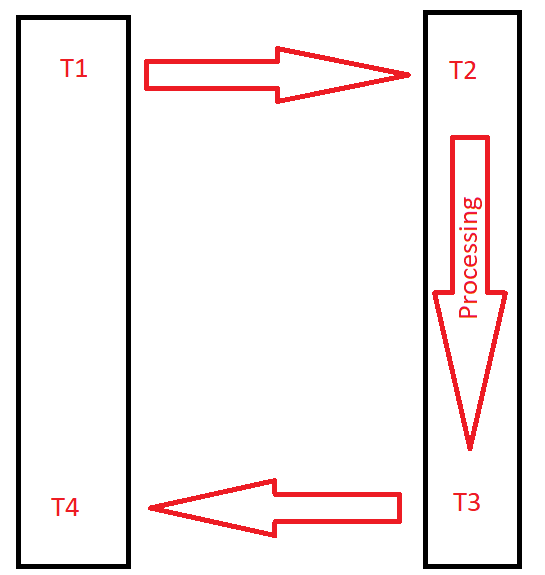
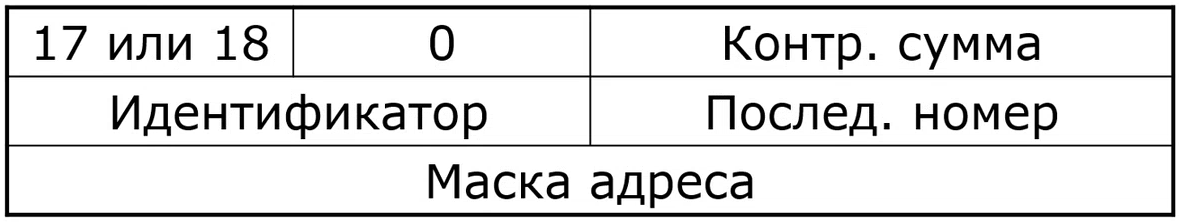
* 4 – подавление источника *(не синхронизирована скорость передачи данных между передатчиком и приемником. Если передатчик слишком быстро передает пакеты, приемная сторона передает следующий пакет. Передающая сторона по умолчанию снижает скорость передачи в 2 раза. Фильтровать нежелательно)*:  
  
  + Тип (4);
  + Последнее поле содержит первую часть пакета, поток которого необходимо замедлить;
* 5 – изменение маршрута *(если пакет с точки зрения маршрутизатора отправляется неоптимальным путем. Отправляет ответ отправителю в качестве совета по перемаршрутизауции)*:  
    
    
  *Легко подделывается. С начала 2000-х фильтруется во всех ОС. По возможности такие пакеты убиваются на всех маршрутизаторах!  
  Проблемы:*  
  *Функция маршрутизации реализуется протоколами маршрутизации, а не ICMP-протоколом (управляющим). Невозможно проконтролировать, кто создал пакет и валидный ли он.*
  + Тип (5);
  + Код *(тип переназначения маршрута)*:
    - 0 – для всей сети,
    - 1 – для узла,
    - 2 – для типа сервиса и сети,
    - 3 – для типа сервиса и узла;
  + IP-адрес маршрутизатора, *куда* необходимо присылать пакеты;
  + Заголовок IP-пакета, который (с точки зрения маршрутизатора-отправителя) идет неоптимальным путем).

## Тестовые и контрольные сообщения

Позволяют проводить диагностику сети.

Обычно идут парами «запрос-ответ».

Типы:

* Запрос эха (8) и ответ на запрос эха (0) *(ping и pong. Проверка работоспособности удаленного узла. Используется в утилитах типа ping и ей подобных, позволяющих проверить достижимость узла в сети)*:  
    
  Идея: станция посылает удаленной станции пакет с типом 8, промежуточные маршрутизаторы доводят его до последней станции. Та, получив его, уничтожает, в ответ формирует такой же пакет с типом 0, а в поле данных копирует те необязательные данные, которые были в поле эхо-запроса, после чего посылает обратно.  
  *Обычно в своей сети разрешаем 8 на выход и 0 на вход. Остальное отрубаем. Иногда – ставим прокси (ICMP-сервер), чтобы он формировал фейковые сообщения за все компьютеры в сети.*
  + Тип (8 или 0);
  + Идентификатор *(для различения пар потоков ping-ов и pong-ов. По нему определяется процесс, которому отдают ответный трафик)*;
  + Последовательный номер *(номер пакета в серии. Для посылки не одного, а нескольких пакетов. Для сопоставления ответа запросу)*;
  + Необязательные данные *(тестирование на прохождение пакетов данных определенного размера по каналу связи. Могут расширить ICMP-пакет до 64 Кб. Большие пакеты могут фильтроваться по размеру из-за имевшей место атаки «ping of death»)*;
* Запрос временной метки (13) и ответ на запрос временной метки (14):  
    
    
  *(позволяют определить временные параметры функционирования сети)*
  + Идентификатор – номер потока сообщений;
  + Последовательный номер – номер пакета в потоке;
  + (T1) **Временная метка отправителя** заполняется источником *(время, когда пакет улетел из отправителя)*;
  + (T2) **Временная метка приема** фиксируется при получении запроса приемником *(время, когда пакет пришел на приемную станцию)*;
  + (T3) **Временная метка передачи** заполняется приемником *(когда был послан ответ)*;
  + (T4) Еще мы знаем время, когда мы получим ответ обратно от приемника;
  + Проблемы:
    - Синхронизация часов;
    - Фильтрация.
* Запрос маски адреса (17) и ответ на запрос маски адреса (18):  
    
  *(Чаще всего – чтобы узнать топологию удаленной сети. Считается опасным, не рекомендуется к использованию вне текущей сети)*.
  + Идентификатор – номер потока сообщений;
  + Последовательный номер – номер пакета в потоке;
  + Маска – записанная маска адреса приемника.

# Адресация приложений. Понятие портов