Протоколы, сервисы и услуги
в Интернет и IP-сетях

Тема № 6
Протокол ICMP

доц. каф. СС и ПД, к.т.н. С. С. Владимиров

2017 г.

Протокол ICMP

ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений)

Сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

Протокол ICMP описан в RFC 792 (с дополнениями в RFC 950, RFC 4884, RFC 6633, RFC 6918) и является стандартом Интернета (STD 5). Протокол ICMP является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. ICMP-пакеты для передачи инкапсулируются в IP-пакеты. Код протокола `0x01`. Текущая версия ICMP для IPv4 называется ICMPv4. В IPv6 существует аналогичный протокол ICMPv6.

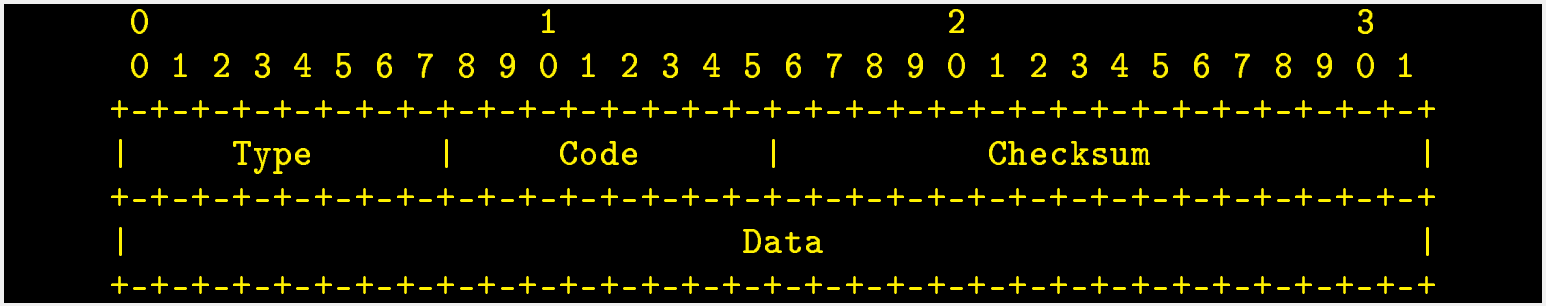
Каждое ICMP-сообщение инкапсулируется непосредственно в пределах одного IP-пакета, и, таким образом ICMP является т. н. «ненадежным» (не контролирующим доставку и её правильность). В отличие от UDP, где реализация надёжности возложена на ПО прикладного уровня, ICMP (в силу специфики применения) обычно не нуждается в реализации надёжной доставки. Тот же Ping, например, служит как раз для проверки потерь IP-пакетов на маршруте.

Правила генерации ICMP-пакетов

- При потере ICMP-пакета никогда не генерируется новый.
- ICMP-пакеты никогда не генерируются в ответ на IP-пакеты с широковещательным или групповым адресом, чтобы не вызывать перегрузку в сети (т. н. «широковещательный шторм»).
- При повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого повреждённого фрагмента, поскольку отправитель всё равно повторит передачу всего IP-пакета целиком.

Формат ICMP-пакета

Формат ICMP-пакета



Type (тип сообщения) и Code (код сообщения)

Эти поля определяют назначение ICMP-пакета (сообщения) и формат поля данных (Data). Поле Type определяет общее назначение сообщения, а поле Code конкретизирует его. Некоторые ICMP-сообщения, предложенные изначально в RFC 792 и некоторых других, впоследствии были признаны устаревшими (не используемыми) и отменены в RFC 6918.

Checksum (контрольная сумма)

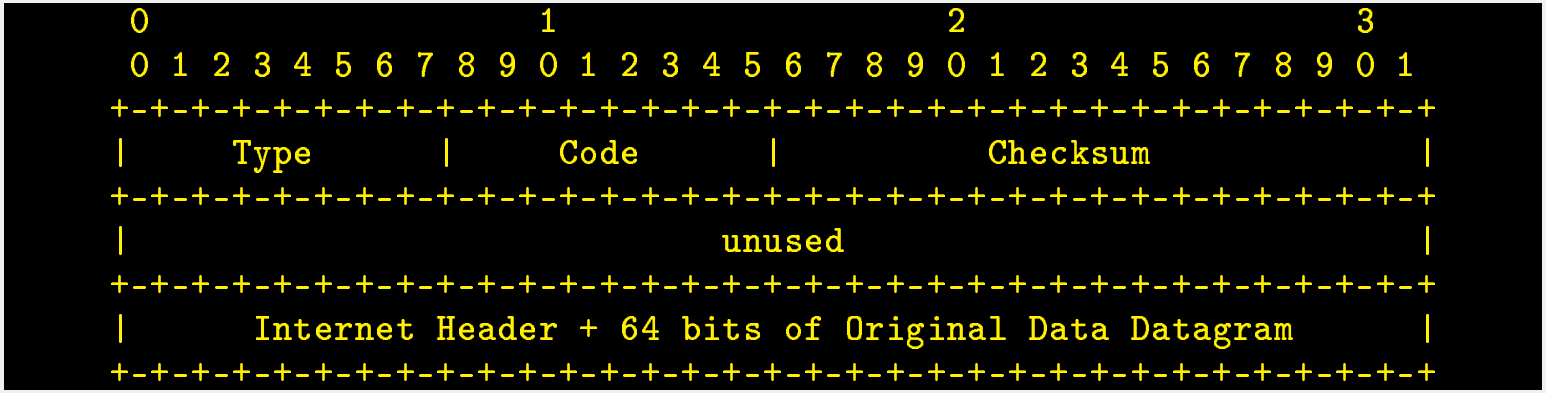
16-битная контрольная сумма, используемая для проверки целостности ICMP-сообщения. Представляет собой 16-битовое поразрядное дополнение суммы всех 16-битовых слов ICMP-сообщения, начиная с поля Type и включая все данные. При вычислении контрольной суммы значение самого поля принимается нулевым.

Data (данные)

Значение этого поля зависит от типа сообщения. Например, для сообщений об ошибках это поле содержит заголовок IP-пакета, вызвавшего ошибку, и первые 64 бита данных.

ICMP-сообщения «Адресат недоступен»

Формат сообщения



Значения полей

`Type` 3

`Code` 0 — сеть недоступна

1 — хост недоступен

2 — неверный протокол

3 — порт закрыт

4 — требуется фрагментация

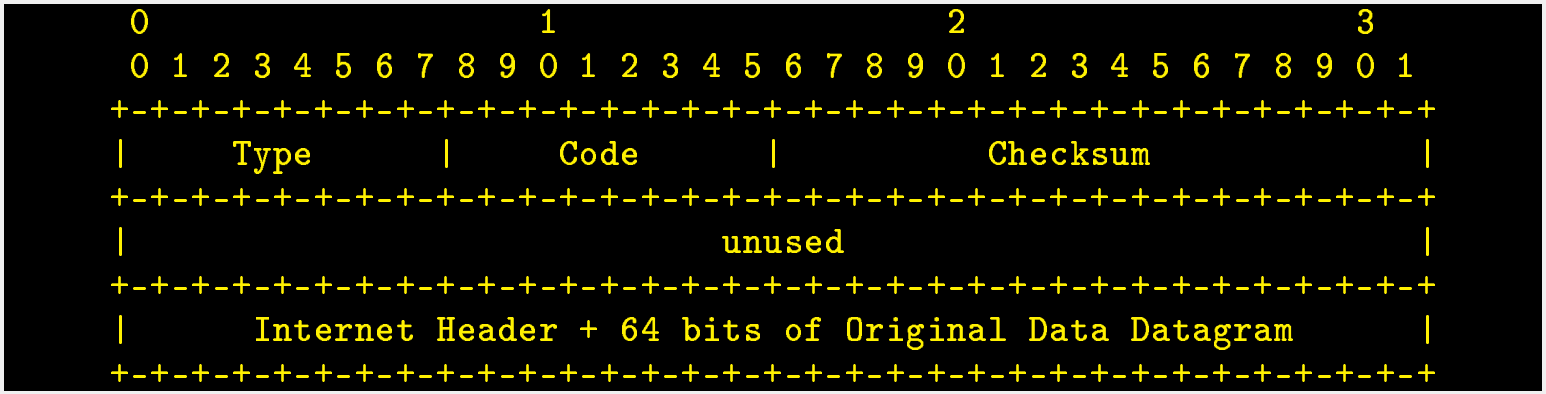
5 — необходима фрагментация, но установлен флаг её запрета (DF)

...

`Data` Содержит 4 неиспользуемых (нулевых) байта, заголовок IP-пакета, вызвавшего ошибку, и первые 64 бита данных.

ICMP-сообщения «Время истекло»

Формат сообщения



Значения полей

`Type` 11

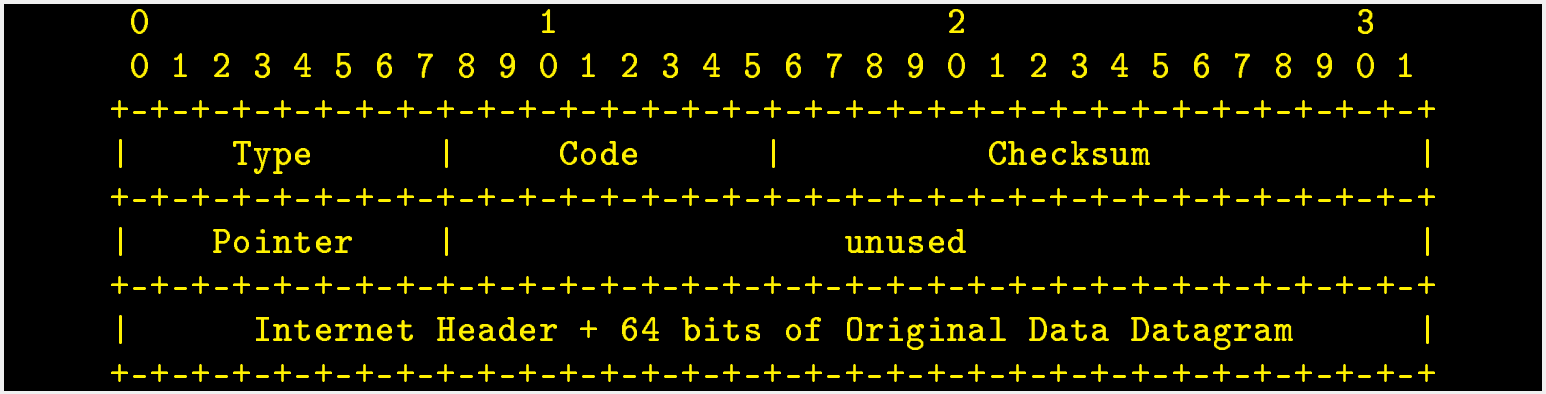
`Code` 0 — время жизни (TTL) истекло

1 — истекло время восстановления пакета при фрагментации

`Data` Содержит 4 неиспользуемых (нулевых) байта, заголовок IP-пакета, вызвавшего ошибку, и первые 64 бита данных.

ICMP-сообщение «Неверный параметр»: ошибка в IP-заголовке

Формат сообщения



Значения полей

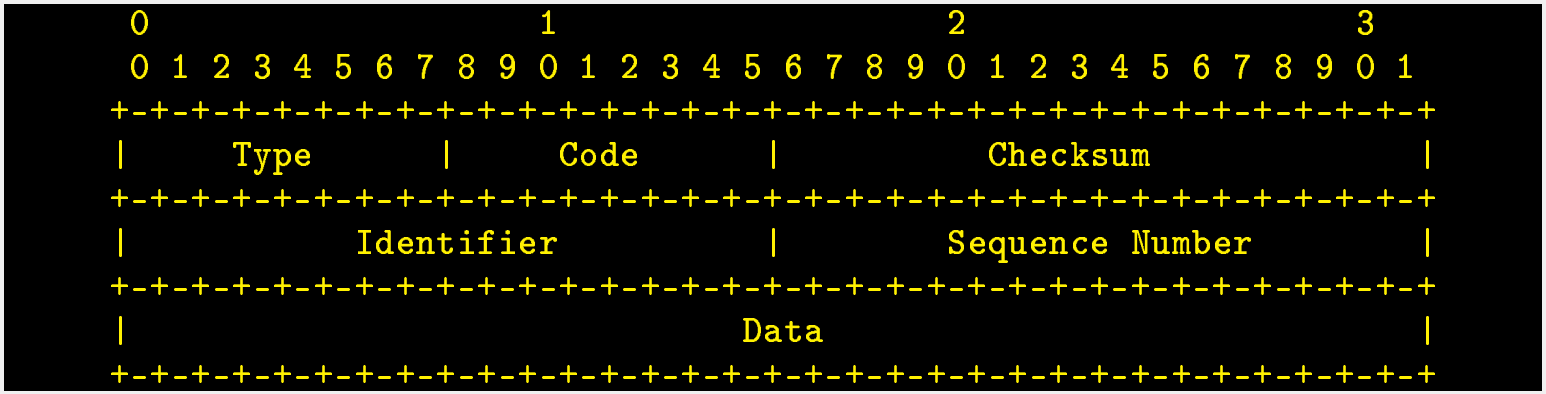
`Type` 12

`Code` 0 — место ошибки указано в поле `Pointer`

`Data` Если `Code=0`, то в поле `Pointer` указывается октет, в котором отмечена ошибка. Далее следуют 3 неиспользуемых (нулевых) байта, заголовок IP-пакета, вызвавшего ошибку, и первые 64 бита данных.

ICMP-сообщения «Эхо-запрос» и «Эхо-ответ»

Формат сообщения



Значения полей

`Type` 12

`Code` 0 — место ошибки указано в поле `Pointer`

`Identifier` Идентификатор последовательности эхо-запросов/эхо-ответов.

`Sequence Number` Номер пакета в последовательности эхо-запросов/эхо-ответов.

`Data` Набор случайных данных для увеличения размера пакета. Зависит от используемого ПО.

ICMP туннелирование

ICMP туннель

Скрытый канал для передачи данных, организованный между двумя узлами, использующий IP-пакеты с типом протокола ICMP (обычно echo request, echo reply). Используется для обхода запретов на передачу информации на межсетевых экранах.

Принцип работы

Узлы обмениваются сообщениями echo request/echo reply, напоминающими работу утилиты ping, однако содержимое сообщений является информацией, передаваемой внутри канала. В случае, если оба узла имеют возможность принимать/отправлять запросы, передача может осуществляться любым узлом, в случае, если один из узлов находится за NAT, он может только отправлять запросы (и получать ответы).

Утилита PingTunnel

Утилита PingTunnel, разработанная Дэниелом Стодлом, позволяет организовать TCP-соединение поверх протокола ICMP или 53 UDP порта.
Для работы PingTunnel необходим запуск прокси-процесса на удаленной машине, имеющей выход в сеть. Пример команд показан ниже.

Прокси: `ptunnel -x пароль`

Клиент: `ptunnel -p хост_прокси -lp лок_порт_туннеля -da адрес_назн -dp порт_назн -x пароль`

Для доступа к адресу и порту назначения необходимо обратиться к заданному порту локального компьютера на loopback интерфейс.

Источники

- Материалы с сайта `https://wikipedia.org/`
- RFC 792. Internet Control Message Protocol
- RFC 6918. Formally Deprecating Some ICMPv4 Message Types
- Проброс TCP соединения через ICMP туннель. URL: `https://www.opennet.ru/tips/1896_proxy_icmp_tunnel.shtml`
- Ping Tunnel. URL: `http://www.cs.uit.no/~daniels/PingTunnel/`