**14 Лекция. Служебные протоколы. Протокол ICMP.**

**Протокол ICMP.**

**ICMP (Internet Control Message Protocol)**- протокол управляющих сообщений.

Вы их получаете постоянно, а иногда и отправляете, например:

* Если адрес не доступен, вы получаете сообщение ICMP.
* Если порт не доступен, вы получаете сообщение ICMP.
* Если вы пользуетесь командой ping, вы получаете сообщение ICMP.
* и т.д.

Сообщение ICMP инкапсулируется прямо в IP пакет (поле данных), т.е. протоколы транспортного уровня не используются.

Поле protocol = 1 (в заголовке IP).

Первый стандарт ICMP определен в RFC0777 (Internet Control Message Protocol J. Postel Apr-01-1981)

Последняя версия - [RFC0792](http://ipm.kstu.ru/internet/doc/rfc/rfc792.txt) (Internet Control Message Protocol J. Postel Sep-01-1981)..

Последняя версия ICMPv6 для IPv6 - [RFC2463](http://ipm.kstu.ru/internet/doc/rfc/rfc2463.txt) (Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering December 1998)

Сообщения делятся на два типа:

* Парные (вопрос/ответ)
* Непарные (например: посылаете запрос к HTTP-серверу, но сервер не доступен, и последний маршрутизатор (или сервер) отправляет ICMP-сообщение (Destination Unreachable) вам)

**Заголовок сообщения ICMP.**

ss

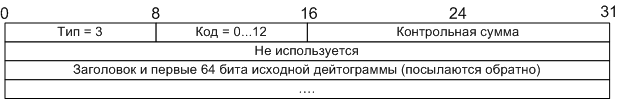
Структура заголовка сообщения ICMP. Слова по 32 бита.

Типы сообщений протокола ICMP

|  |  |  |
| --- | --- | --- |
| **Тип** | **Сообщение** | **Назначение** |
| 0 | Echo Reply | Ответ ICMP - эхо (ping) |
| 3 | Destination Unreachable | Цель не достижима |
| 4 | Source Quench | Переполнение очереди источника |
| 5 | Redirect | Перенаправление маршрута |
| 8 | Echo Request | Запрос ICMP - эхо (ping) |
| 9 |  | Объявление маршрутизатора |
| 10 |  | Запрос маршрутизатора |
| 11 | Time Exceeded | Время жизни истекло |
| 12 | Parameter Problem | Неверный параметр |
| 13 | Timestamp Request | Запрос метки времени |
| 14 | Timestamp Reply | Ответ метки времени |
| 15 | Information Request | Запрос информации |
| 16 | Information Reply | Ответ информации |
| 17 | Address Mask Request | Запрос маски адреса |
| 18 | Address Mask Reply | Ответ маски адреса |

**Сообщение Destination Unreachable**

Непарное сообщение, формируется, если цель недостижима.



Структура сообщения ICMP - Destination Unreachable

"Заголовок и первые 64 бита исходной дейтограммы" отправляются для диагностики причины ошибки.

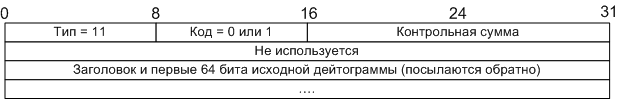
Диагностические коды сообщений Destination Unreachable

|  |  |  |
| --- | --- | --- |
| **Код** | **Тип кода** | **Значение** |
| 0 | Network Unreachable | Сеть назначения недостижима |
| 1 | Host Unreachable | Хост назначения не достижим |
| 2 | Protocol Unreachable | Протокол недостижим |
| 3 | Port Unreachable | Порт недостижим |
| 4 | Fragmentation Need & DF set | Необходима фрагментация, однако она запрещена |
| 5 | Source Route Failed | Исходный маршрут вышел из строя |
| 6 | Destination Network Unknown | Сеть назначения неизвестна |
| 7 | Destination Host Unknown | Хост назначения неизвестен |
| 8 | Source Host Isolated | Источник изолирован |
| 9 | Communication with destination Network Administratively Prohibited | Взаимодействие с сетью назначения запрещено |
| 10 | Communication with destination Host Administratively Prohibited | Взаимодействие с узлом назначения запрещено |
| 11 | Network Unreachable for type of service | Сеть назначения недоступна для запрошенного типа сервиса |
| 12 | Host Unreachable for type of service | Хост назначения недоступен для запрошенного типа сервиса |
| 13 |  | Связь административно запрещена с помощью фильтра |
| 14 |  | Нарушение старшинства ЭВМ |
| 15 |  | Дискриминация по старшинству |

Из таблицы видно, что коды 2 и 3 формируются сервером назначения.

**Сообщение Time Exceeded**

Непарное сообщение, формируется, если время жизни истекло.



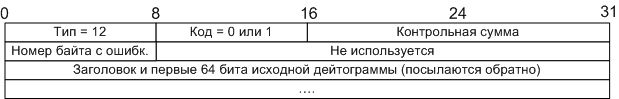
Структура сообщения ICMP - Time Exceeded

Диагностические коды сообщений Time Exceeded

|  |  |
| --- | --- |
| **Код** | **Значение** |
| 0 | Время жизни = 0 |
| 1 | Таймер дефрагментации установился в 0 до полной сборки принятого сообщения |

**Сообщение Parameter Problem**

Непарное сообщение, формируется, если заголовок IP-дейтограммы содержит неверный параметр.



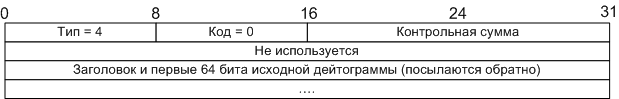
Структура сообщения ICMP - Parameter Problem

Диагностические коды сообщений Parameter Problem

|  |  |
| --- | --- |
| **Код** | **Значение** |
| 0 | Если возникла проблема с интерпретацией какого то поля (используется поле "номер байта с ошибкой в исходном сообщении") |
| 1 | Если возникла проблема с несоответствием какого то запрашиваемого параметра, с установленными требованиями |

**Сообщение Source Quench**

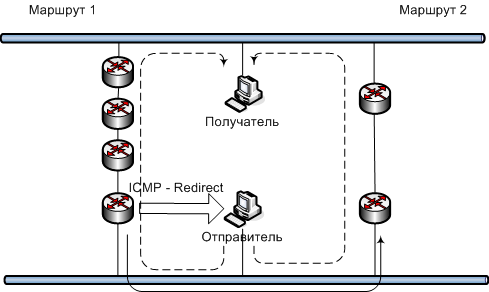
Непарное сообщение, формируется, если возникла перегрузка маршрутизатора, пакет не может быть помещен в буфер, т.к. он переполнен.



Структура сообщения ICMP - Source Quench

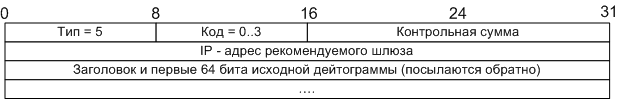
**Сообщение Redirect**

Непарное сообщение, формируется, если изменен маршрут для пакета.



Случай, когда маршрутизатор перенаправляет пакеты по другому маршруту (маршрут 2).

И предлагает в сообщении ICMP изменить шлюз по умолчанию



Структура сообщения ICMP - Redirect

Диагностические коды сообщений Redirect

|  |  |  |
| --- | --- | --- |
| **Код** | **Тип кода** | **Значение** |
| 0 | Redirect Datagram for networks | Изменение маршрута для сети |
| 1 | Redirect Datagram for host | Изменение маршрута для хоста |
| 2 | Redirect Datagram for the Type of service and networks | Изменение маршрута для типа сервиса или сети |
| 3 | Redirect Datagram for the Type of service and host | Изменение маршрута для типа сервиса или хоста |

**Сообщение Echo Request/Echo Reply**

Парное сообщение. Любой узел, получивший Echo Request, должен ответить Echo Reply отправителю.

Echo Request сообщения формирует программа **ping.**



Структура сообщения ICMP - Echo Request/Echo Reply

Идентификатор и последовательный номер используются для определения, какой ответ принадлежит какому запросу.

**Атаки с помощью Echo Request/Echo Reply**

Можно осуществить DoS-атаку (Denial of Service - подавление услуги).

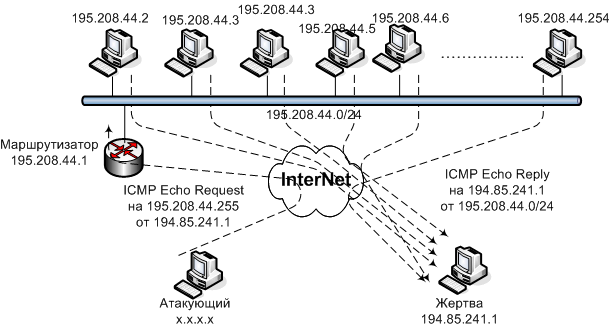
Цель: загрузить сервер так, чтобы он не мог отвечать.

Нужно послать как можно больше ответов Echo Reply на жертву.

Для этого можно задействовать чужие сети.

Алгоритм:

1. Указываем адрес источника - адрес жертвы (194.85.241.1)
2. Указываем адрес получателя - адрес типа Directed Broadcast (195.208.44.255), на этот адрес должны ответить все узлы сети 195.208.44.0/24
3. Посылаем сообщение Echo Request.
4. 253 машины посылают ответ на жертву (194.85.241.1)
5. Все повторяем много раз, а лучше задействовать побольше таких сетей.
6. Жертва будет перегружена.



Атаки с помощью Echo Request/Echo Reply

Меры предотвращения таких атак:

* Запретить прием и распространение сообщений типа Directed Broadcast.
* Уничтожать сфальсифицированные пакеты, сопоставляя IP источника с маршрутной таблицей и номером интерфейса, с которого получен пакет.
* Запретить трафик ICMP (ping, traceroute и т.д., работать не будут).

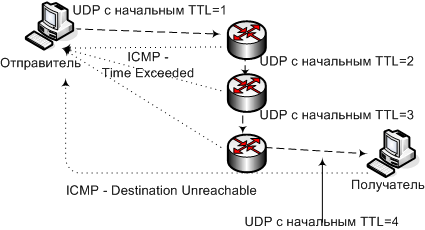
**Принцип работы traceroute**

traceroute отправляет на несуществующий порт удаленного узла последовательность UDP-дейтаграмм, .

Номер используемого порта по умолчанию 33434.

Алгоритм работы:

* Посылаются дейтограммы с TTL=1 (время жизни пакета)
* Первый же маршрутизатор уменьшает TTL на 1, т.е. TTL=0 и пакет уничтожается, а отправителю посылается ICMP сообщение Time Exceeded.
* Посылаются дейтограммы с TTL=2 (время жизни пакета)
* Первый же маршрутизатор уменьшает TTL на 1, т.е. TTL=1 и пакет проходит дальше.
* Второй маршрутизатор уменьшает TTL на 1, т.е. TTL=1 и пакет уничтожается, а отправителю посылается ICMP сообщение Time Exceeded.
* И т.д.
* Попадая на получателя, пакет уничтожается, т.к. получатель не знает, что с ним делать (порт не существует), и отправителю посылается ICMP сообщение Destination Unreachable.



Пример работы traceroute