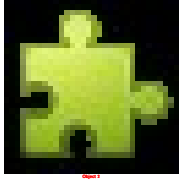

Протокол ICMP

Можно представить ряд ситуаций, когда протокол IP не может доставить пакет адресату, например истекает время жизни пакета, в таблице маршрутизации отсутствует маршрут к заданному в пакете адресу назначения, пакет не проходит проверку по контрольной сумме, шлюз не имеет достаточно места в своем буфере для передачи какого-либо пакета и т. д., и т. п.

Как мы не раз отмечали, протокол IP доставляет данные, руководствуясь принципом «по возможности», то есть не предпринимает мер для гарантированной передачи данных адресату. Это свойство «необязательности» протокола IP компенсируется протоколами более высоких уровней стека TCP/IP, например TCP на транспортном уровне и в какой-то степени DNS на прикладном уровне. Они берут на себя обязанности по обеспечению надежности, применяя такие известные приемы, как нумерация сообщений, подтверждение доставки, повторная посылка данных.

Протокол ICMP также служит дополнением, компенсирующим ненадежность протокола IP, но несколько другого рода. Он не предназначен для исправления возникших при передаче пакета проблем: если пакет потерян, ICMP не может послать его заново. Задача ICMP другая — он является средством оповещения отправителя о «несчастных случаях», произошедших с его пакетами. Пусть, например, протокол IP, работающий на каком-либо маршрутизаторе, обнаружил, что пакет для дальнейшей передачи по маршруту необходимо фрагментировать, но в пакете установлен признак DF (не фрагментировать). Протокол IP, обнаруживший, что он не может передать IP-пакет далее по сети, прежде чем отбросить пакет, должен отправить диагностическое ICMP-сообщение конечному узлу-источнику.

Для передачи по сети ICMP-сообщение инкапсулируется в поле данных IP-пакета. IP-адрес узла-источника определяется из заголовка пакета, вызвавшего инцидент.

Сообщение, прибывшее в узел-источник, может быть обработано там либо ядром операционной системы, либо протоколами транспортного и прикладного уровней, либо приложениями, либо просто проигнорированы. Важно, что обработка ICMP-сообщений не входит в обязанности протоколов IP и ICMP.

Заметим, что некоторые из пакетов могут исчезнуть в сети, не вызвав при этом никаких оповещений. В частности, протокол ICMP не предусматривает передачу сообщений о проблемах, возникающих при обработке IP-пакетов, несущих ICMP-сообщения об ошибках. Такое решение было принято разработчиками протокола, чтобы не порождать «штормы» в сетях, когда количество сообщений об ошибках лавинообразно возрастает.

Особенностью протокола ICMP является функциональное разнообразие решаемых задач, а следовательно, и связанных с этим сообщений. Все типы сообщений имеют один и тот же формат (рис. 1), однако интерпретация полей существенно зависит от того, к какому типу относится сообщение.

Рис. 1. Формат ICMP-сообщения

Заголовок ICMP-сообщения состоит из 8 байт:

- тип (1 байт) — числовой идентификатор типа сообщения;
- код (1 байт) — числовой идентификатор, более тонко дифференцирующий тип ошибки;
- контрольная сумма (2 байта) — подсчитывается для всего ICMP-сообщения.

Содержимое оставшихся четырех байтов в заголовке и поле данных зависит от значений полей типа и кода.

На рис. 2 показана таблица основных типов ICMP-сообщений. Эти сообщения можно разделить на две группы (помеченные на рисунке условными символами):

- сообщения об ошибках;
- сообщения запрос-ответ.

Сообщения типа запрос-ответ связаны в пары: эхо-запрос — эхо-ответ, запрос маски -ответ маски, запрос времени — ответ времени. Отправитель сообщения-запроса всегда рассчитывает на получение соответствующего сообщения-ответа.

Рис. 2. Типы и коды ICMP-сообщений

Сообщения, относящиеся к группе сообщений об ошибках, конкретизируются уточняющим кодом. На рисунке показан фрагмент таблицы кодов для сообщения об ошибке недостижимости узла назначения, имеющей тип 3. Из таблицы мы видим, что это сообщение может быть вызвано различными причинами, такими как неверный адрес сети или узла (код О или 1), отсутствием на конечном узле-адресате необходимого протокола прикладного уровня (код 2 — «протокол недостижим») или открытого порта UDP/TCP (код 3 — «порт недостижим»). Узел (или сеть) назначения может быть также недостижим по причине временной неработоспособности аппаратуры или из-за того, что маршрутизатор не имеет данных о пути к сети назначения. Всего таблица содержит 15 кодов. Аналогичные таблицы кодов существуют и для других типов сообщений об ошибках.

Утилита ping

А сейчас давайте рассмотрим представителей другой группы ICMP-сообщений — эхо-запросы и эхо-ответы и поговорим об использовании этих сообщений в известной утилите ping.

Эхо-запрос и эхо-ответ, в совокупности называемые эхо-протоколом, представляют собой очень простое средство мониторинга сети. Компьютер или маршрутизатор посылает по составной сети ICMP-сообщение эхо-запроса, указывая в нем IP-адрес узла, достижимость которого нужно проверить. Узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса. Так как эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, то их успешная доставка означает нормальное функционирование всей транспортной

системы составной сети.

Формат эхо-запроса и эхо-ответа показан на рис. 1. Поле типа для эхо-ответа равно 0, для эхо-запроса — 8; поле кода всегда равно 0 и для запроса, и для ответа. В байтах 5 и 6 заголовка содержится идентификатор запроса, в байтах 7 и 8 — порядковый номер. В поле данных эхо-запроса может быть помещена произвольная информация, которая в соответствии с данным протоколом должна быть скопирована в поле данных эхо-ответа.

Рис. 1. Формат ICMP-сообщений типа эхо-запрос и эхо-ответ

```
# ping serverl.citmgu.ru
Pinging serverl.citmgu.ru [193.107.2.200] with 64 bytes of data
Reply from 193.107.2.200
Reply from 193Л07.2.200
Reply from 193.107.2.200
Reply from 193.107.2.200
bytes=64 time=256ms TTL= 123
bytes=64 time=310ms TTL= 123
bytes=64 time=260ms TTL= 123
bytes=64 time=146ms TTL= 123
```

Из приведенной распечатки видно, что в ответ на тестирующие запросы, посланные узлу serveM .mgu.ru, было получено 4 эхо-ответа. Длина каждого сообщения составляет 64 байта. В следующей колонке помещены значения времени оборота (RTT), то есть времени от момента отправки запроса до получения ответа на этот запрос. Как видим, сеть работает достаточно нестабильно — время в последней строке отличается от времени во второй более чем в два раза. На экран выводится также оставшееся время жизни поступивших пакетов.

Утилита traceroute

В качестве примера рассмотрим использование сообщений об ошибках в популярной утилите мониторинга сети traceroute.

Когда маршрутизатор не может передать или доставить IP-пакет, он отсылает узлу, отправившему этот пакет, сообщение о недостижимости узла назначения. Формат этого сообщения показан на рис. 1. В поле типа помещается значение 3, а в поле кода — значение

из диапазона 0-15, уточняющее причину, по которой пакет не был доставлен. Следующие за полем контрольной суммы четыре байта заголовка не используются и заполняются , нулями.

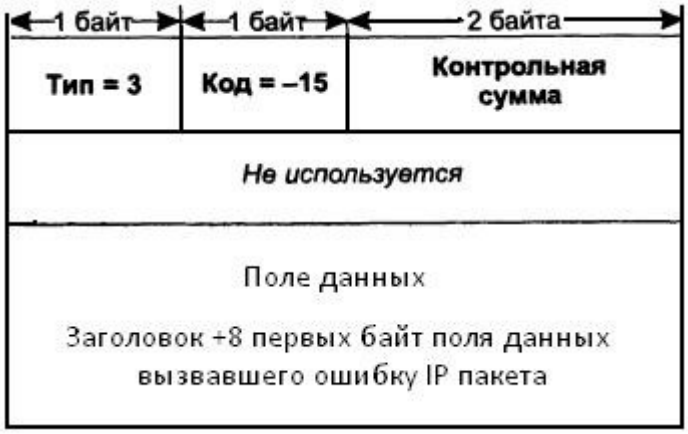

Рис. 1. Формат ICMP-сообщения об ошибке недостижимости узла назначения

Помимо причины ошибки, указанной в заголовке (в полях типа и кода), дополнительная диагностическая информация передается в поле данных ICMP-сообщения. Именно туда помещается заголовок IP и первые 8 байт данных того IP-пакета, который вызвал ошибку.

Эта информация позволяет узлу-отправителю еще точнее диагностировать причину ошибки. Это возможно, так как все протоколы стека TCP/IP, использующие для передачи своих сообщений IP-пакеты, помещают наиболее важную для анализа информацию в первые 8 байт своих сообщений. В частности, ими вполне могут оказаться первые 8 байт заголовка TCP или UDP, в которых содержится информация (номер порта), идентифицирующая приложение, пославшее потерянный пакет. Следовательно, при разработке приложения можно предусмотреть встроенные средства реакции на сообщения о недоставленных пакетах.

ЮМР-сообщения об ошибках лежат в основе работы популярной утилиты traceroute для Unix, имеющей в Windows название tracert. Эта утилита позволяет проследить маршрут до удаленного хоста, определить среднее время оборота (RTT), IP-адрес и в некоторых случаях доменное имя каждого промежуточного маршрутизатора. Такая информация помогает найти маршрутизатор, на котором обрывается путь пакета к удаленному хосту.

Утилита traceroute осуществляет трассировку маршрута, посылая серию обычных IP пакетов в конечную точку изучаемого маршрута. Идея метода состоит в следующем. Значение времени жизни (TTL) первого отправляемого пакета устанавливается равным 1. Когда протокол IP первого маршрутизатора принимает этот пакет, то он в соответствии со своим алгоритмом уменьшает значение TTL на 1 и получает 0. Маршрутизатор отбрасывает пакет с нулевым временем жизни и возвращает узлу-источнику ICMP-сообщение об ошибке истечения времени дейтаграммы (значение поля типа равно 11) вместе с заголовком IP и первыми 8 байтами потерянного пакета.

Затем traceroute посылает следующий IP-пакет, но теперь со значением TTL, равным 2. Этот пакет благополучно проходит первый маршрутизатор, но «умирает» на втором, о чем немедленно отправляется аналогичное ICMP-сообщение об ошибке истечения времени дейтаграммы. Утилита traceroute запоминает адрес второго маршрутизатора и т. д. Такие

действия выполняются с каждым маршрутизатором вдоль маршрута вплоть до узла назначения или неисправного маршрутизатора. Мы рассматриваем работу утилиты traceroute весьма схематично, но и этого достаточно, чтобы оценить изящество идеи, лежащей в основе ее работы. Остальные ICMP-сообщения об ошибках имеют такой же формат и отличаются друг от друга только значениями полей типа и кода.

Далее приведена копия экранной формы, выведенной утилитой tracert (Windows) при трассировке хоста ds.jnternic.net [198.49.45.29]:

```
1 311 ms 290 ms 261 ms 144.206.192.100
2 281 ms 300 ms 271 ms 194.85.73.5
3 2023 ms 290 ms 311 ms moscow-m9-2-S5.relcom.eu.net [193.124.254.37]
4 290 ms 261 ms 280 ms MSK-M9-13.Relcom.EU.net [193.125.15.13]
5 270 ms 281 ms 290 ms MSK.RAIL-l-ATM0-155Mb.Relcom.EU.net [193.124.254.82]
6 300 ms 311 ms 290 ms SPB-RASC0M-l-E3-l-34Mb.Relcom.EU.net [193.124.254.78]
7 311 ms 300 ms 300 ms Hssill-0.GW1.STK2.ALTER.NET [146.188.33.125]
8 311 ms 330 ms 291 ms 421.ATM6-0-0.CR2.STK2.Alter.Net [146.188.5.73]
9 360 ms »331 ms 330 ms 219.Hssi4-0.CR2.LND1.Alter.Net [146.188.2.213]
10 351 ms 330 ms 331 ms 412.Atm5-0.BRl.LNDl.Alter.net [146.188.3.205]
11 420 ms 461 ms 420 ms 167.ATM8-0-0.CR1.ATLI.Alter.Net [137.39.69.182]
12 461 ms 441 ms 440 ms 311.ATM12-0-0.BR1.ATL1.Alter.Net [137.39.21.73]
13 451 ms 410 ms 431 ms atlantal-brl.bbnplanet.net [4.0.2.141]
14 420 ms 411 ms 410 ms viennal-br2.bbnplanet.net [4.0.3-.154]
15 411 ms 430 ms 2514 ms viennal-nbr3.bbnplanet.net [4.0.3.150]
16 430 ms 421 ms 441 ms viennal-nbr2.bbnplanet.net [4.0.5.45]
17 431 ms 451 ms 420 ms cambridgel-brl.bbnplanet.net [4.0.5.42]
18 450 ms 461 ms 441 M C cambridgel-crl4.bbnplanet.net [4.0.3.94]
19 451 M C 461 M C 460 M C attbcstoll.bbnplanet.net [206.34.99.38]
20 501 M C 460 M C 481 M C shutdown.ds.internic.net [198.49.45.29]
```

Последовательность строк соответствует последовательности маршрутизаторов, образующих маршрут к заданному узлу. Первое число в строке — число хопов до соответствующего маршрутизатора. Утилита traceroute тестирует каждый маршрутизатор трижды, поэтому следующие три числа в строке — это значения RTT, вычисленные путем посылки трех пакетов, время жизни которых истекло на этом маршрутизаторе. Если ответ от какого-либо маршрутизатора не приходит за заданное время, то вместо времени на экране печатается звездочка (*).

Далее идут IP-адрес и доменное имя (если оно имеется) маршрутизатора. Видно, что почти все интерфейсы маршрутизаторов поставщиков услуг Интернета зарегистрированы в службе DNS, а первые два, относящиеся к локальным маршрутизаторам, — нет.

Еще раз подчеркнем, что время, указанное в каждой строке, это не время прохождения пакетов между двумя соседними маршрутизаторами, а время, за которое пакет проделывает путь от источника до соответствующего маршрутизатора и обратно. Так как ситуация в Интернете с загрузкой маршрутизаторов постоянно меняется, то время достижимости маршрутизаторов не всегда нарастает монотонно, а может изменяться достаточно произвольным образом.

Формат пакета ICMP

Октет	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0—3	Тип								Код								Контрольная сумма															

… Данные (формат зависит от значений полей «Код» и «Тип»)

Типы пакетов ICMP

Тип	Код	Сообщение	Данные (длина, бит)
0	0	Эхо-ответ Идентификатор (16) Номер последовательности (16) Данные (переменная)	
1, 2		Зарезервировано	
3		Адресат недоступен Не используется (32) Заголовок IP, Начало исходной дейтаграммы (64)	
	0	Сеть недостижима	
	1	Узел недостижим	
	2	Протокол недостижим	
	3	Порт недостижим	
	4	Необходима фрагментация, но установлен флаг её запрета (DF)	
	5	Неверный маршрут от источника	
	6	Сеть назначения неизвестна	
	7	Узел назначения неизвестен	
	8	Узел источник изолирован	
	9	Сеть административно запрещена	
	10	Узел административно запрещён	
	11	Сеть недоступна для ToS	
	12	Узел недоступен для ToS	
	13	Коммуникации административно запрещены	
	14	Нарушение порядка предпочтения узлов	
	15	Активно отсечение порядка предпочтения	
4	0	Сдерживание источника (отключение источника при переполнении очереди)	
5		Перенаправление Адрес маршрутизатора (32) Заголовок IP, Начало исходной дейтаграммы (64)	
	0	Перенаправление пакетов в сеть	
	1	Перенаправление пакетов к узлу	
	2	Перенаправление для каждого типа обслуживания (ToS)	
	3	Перенаправление пакета к узлу для каждого типа обслуживания	
6	0	Альтернативный адрес узла	
7		Зарезервировано	
8	0	Эхо-запрос	

		Идентификатор (16)	Номер последовательности (16)
		Данные (переменная)	
9	0	Объявление маршрутизатора Количество адресов (8) / Размер элемента (8) / Срок действия (16) Адрес[1] (32) Предпочтительность[1] (32) … Адрес[N] (32) Предпочтительность[N] (32)	
10	0	Запрос маршрутизатора Не используется (32)	
11		Время жизни дейтаграммы истекло Не используется (32) Заголовок IP, Начало исходной дейтаграммы (64)	
	0	Время жизни пакета (TTL) истекло при транспортировке	
	1	Время жизни пакета истекло при сборке фрагментов	
12		Неверный параметр (проблема с параметрами дейтаграммы: ошибка в IP-заголовке или отсутствует необходимая опция) Указатель говорит об ошибке Указатель (8) / Не используется (24) Заголовок IP, Начало исходной дейтаграммы (64)	
	1	Отсутствует требуемая опция Не используется (32) Заголовок IP, Начало исходной дейтаграммы (64)	
	2	Некорректная длина	
13	0	Запрос метки времени Идентификатор (16) / Номер последовательности (16) Начальное время (32) Время приёма (32) Время отправки (32)	
14	0	Ответ с меткой времени	
15	0	Информационный запрос Идентификатор (16) / Номер последовательности (16)	
16	0	Информационный ответ	
17	0	Запрос адресной маски Идентификатор (16) / Номер последовательности (16) Маска (32)	
18	0	Отклик на запрос адресной маски	
19		Зарезервировано (для обеспечения безопасности)	

20—29	Зарезервировано (для экспериментов на устойчивость к ошибкам)	
	Трассировка маршрута	
30	Идентификатор (16)	Не используется (16)
	Количество хопов исходящего пакета (16)	Количество хопов возвращающегося пакета (16)
	Скорость линии связи (32)	
	MTU линии связи (32)	
	0	Исходящий пакет успешно отправлен
	1	Путь для исходящего пакета не найден, пакет уничтожен
	Ошибка преобразования датаграммы	
31	Указатель (32)	
	Заголовок IP и транспортного протокола исходной дейтаграммы	
	0	Неизвестная или неуказанная ошибка
	1	Невозможно конвертировать опцию
	2	Неизвестная обязательная опция
	3	Неподдерживаемая обязательная опция
	4	Неподдерживаемый транспортный протокол
	5	Превышена полная длина
	6	Превышена длина заголовка IP
	7	Номер транспортного протокола больше 255
	8	Номер порта вне допустимого диапазона
	9	Превышена длина заголовка транспортного протокола
	10	Переход через границу 32 бит и установлен бит ACK
	11	Неизвестная обязательная опция транспортного протокола
32	Перенаправление для мобильного узла	
33	IPv6 Where-Are-You (где вы находитесь)	
34	IPv6 I-Am-Here (я здесь)	
35	Запрос перенаправления для мобильного узла	
36	Отклик на запрос перенаправления для мобильного узла	
37	Запрос доменного имени	
38	Ответ на запрос доменного имени	
39	Обнаружение алгоритма безопасности SKIP (SKIP algorithm discovery ICMP message)	
	Photuris	
40	0	Зарезервировано
	1	Неизвестный индекс параметров безопасности
	2	Параметры безопасности верны, но произошла ошибка аутентификации
	3	Параметры безопасности верны, но произошёл сбой при расшифровке
	4	Требуется проверка подлинности
	5	Требуется авторизация
41—	Зарезервировано	

252	
253-254	Зарезервировано для экспериментов по RFC 3692
255	Зарезервировано

Правила генерации ICMP-пакетов

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