2. Протокол мониторинга ICMP

Протокол передачи команд и сообщений об ошибках (ICMP - internet control message protocol) выполняет многие и не только диагностические функции, хотя у рядового пользователя именно этот протокол вызывает раздражение, сообщая об его ошибках или сбоях в сети. Именно этот протокол используется программным обеспечением ЭВМ при взаимодействии друг с другом в рамках идеологии TCP/IP. Осуществление повторной передачи пакета, если предшествующая попытка была неудачной, лежит на TCP или прикладной программе. При пересылке пакетов промежуточные узлы не информируются о возникших проблемах, поэтому ошибка в маршрутной таблице будет восприниматься как неисправность в узле адресата и достоверно диагностироваться не будет. ICMP-протокол сообщает об ошибках в IP-дейтограммах, но не дает информации об ошибках в самих ICMP-сообщениях. icmp использует IP, а IP-протокол должен использовать ICMP. В случае ICMP-фрагментации сообщение об ошибке будет выдано только один раз на дейтограмму, даже если ошибки были в нескольких фрагментах.

Задачи, решаемые ICMP:
Подводя итоги, можно сказать, что ICMP-протокол осуществляет:

- передачу отклика на пакет или эхо на отклик;
- контроль времени жизни дейтограмм 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.

ICMP-сообщения об ошибках никогда не выдаются в ответ на:

- ICMP-сообщение об ошибке.
- При мультикаст или широковещательной адресации.
- Для фрагмента дейтограммы (кроме первого).
- Для дейтограмм, чей адрес отправителя является нулевым, широковещательным или мультикаст.

Эти правила призваны блокировать потоки дейтограмм, посылаемым в отклик на мультикаст или широковещательные ICMP-сообщения.

ICMP-сообщения имеют свой формат, а схема их вложения аналогична UDP или TCP и представлена на рис. 4

Рис. 4. Схема вложения ICMP-пакетов в Ethernet-кадр

Все ICMP пакеты начинаются с 8-битного поля типа ICMP и его кода (15 значений). Код уточняет функцию ICMP-сообщения. Таблица этих кодов приведена ниже (символом * помечены сообщения об ошибках, остальные - являются запросами)

Таблица 1. Описание ICMP-сообщений

ICMP-сообщение		Описание сообщения
	К	
0		Эхо-ответ (ping-отклик)
3		Адресат недостижим
	0	* Сеть недостижима
	1	* ЭВМ не достижима
	2	* Протокол не доступен
	3	* Порт не доступен
	4	* Необходима фрагментация сообщения
	5	* Исходный маршрут вышел из строя
	6	* Сеть места назначения не известна
	7	* ЭВМ места назначения не известна
	8	* Исходная ЭВМ изолирована
	9	* Связь с сетью места назначения административно запрещена
	10	* Связь с ЭВМ места назначения административно запрещена
	11	* Сеть не доступна для данного вида сервиса
	12	* ЭВМ не доступна для данного вида сервиса
	13	* Связь административно запрещена с помощью фильтра.
	14	* Нарушение старшинства ЭВМ
	15	* Дискриминация по старшинству
4	0	* Отключение источника при переполнении очереди (quench)
5		Переадресовать (изменить маршрут)
	0	Переадресовать дейтограмму в сеть (устарело)
	1	Переадресовать дейтограмму на ЭВМ
	2	Переадресовать дейтограмму для типа сервиса (tos) и сети
	3	Переадресовать дейтограмму для типа сервиса и ЭВМ
8	0	Эхо запроса (ping-запрос).
9	0	Объявление маршрутизатора
10	0	Запрос маршрутизатора

11		Для дейтограммы время жизни истекло (ttl=0):
	0	*при передаче
	1	* при сборке (случай фрагментации).
12		* Проблема с параметрами дейтограммы
	0	* Ошибка в ip-заголовке
	1	* Отсутствует необходимая опция
13		Запрос временной метки
14		Временная метка-отклик
15		Запрос информации (устарел)
16		Информационный отклик (устарел)
17		Запрос адресной маски
18		Отклик на запрос адресной маски

Рис. 5. Форматы пакетов ICMP

Рис. 6. Эхо-запрос и отклика ICMP

Поля **Идентификатор** (обычно это идентификатор процесса) и **Номер по порядку** (увеличивается на 1 при посылке каждого пакета) служат для того, чтобы отправитель мог связать в пары запросы и отклики.

Поле **Тип** определяет, является ли этот пакет запросом (8) или откликом (0).

Поле **Контрольная сумма** представляет собой 16-разрядное дополнение всего ICMP-сообщения, начиная с поля Тип.

Поле **Данные** служит для записи информации, возвращаемой отправителю.

При выполнении процедуры ping эхо-запрос с временной меткой в поле данные посылается адресату. Если адресат активен, он принимает IP-пакет, меняет адрес отправителя и получателя местами и посылает его обратно. ЭВМ-отправитель, восприняв этот отклик, может сравнить временную метку, записанную им в пакет, с текущим показанием внутренних часов и определить время распространения пакета (RTT - round trip time). Размер поля Данные не регламентирован и определяется предельным размером IP-пакета.

Так как в пакете ICMP нет поля порт, то при запуске нескольких процессов PING одновременно может возникнуть проблема с тем какому из процессов следует передать тот или иной отклик. Для преодоления этой неопределенности следует использовать уникальные значения полей Идентификатор.

Поле **Идентификатор** бывает важно, когда ЭВМ использует программируемый генератор трафика. В этом случае очередной ICMP-пакет посылается, не дожидаясь прихода отклика. Более того, такие пакеты могут генерироваться несколькими процессами одновременно. В этом случае поле Идентификатор становится необходимым, чтобы определить, какому процессу ОС передать очередной отклик.