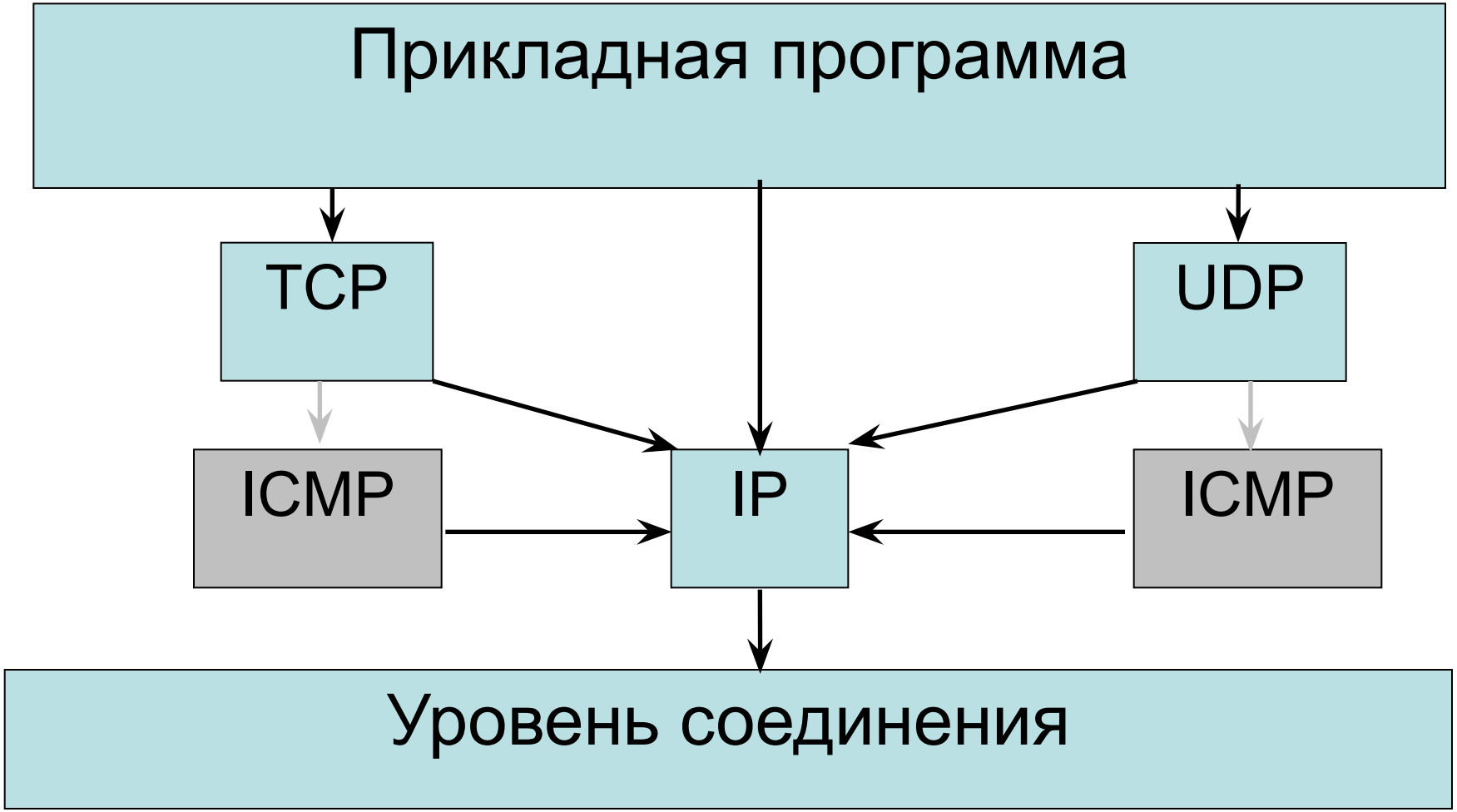
ICMP
межсетевой протокол управляющих сообщений

Выполнил: студент группы СУ-61
Французов Виталий

Межсетевой протокол управляющих сообщений ICMP (Internet Control Message Protocol) играет роль транспортного протокола для управляющей и диагностической информации, которой обмениваются между собой IP-, TCP- или UDP-модули скрытно от приложений.

Место ICMP при пересылке данных



Заголовок ICMP-пакета

Тип

Однобайтовое поле, содержащее идентификатор типа ICMP-пакета. Значение этого поля определяет формат всех остальных данных в датаграмме. Возможные значения этого поля:

0	Ответ на запрос эха
3	Адресат недоступен
4	Подавление источника
5	Перенаправление
8	Запрос эха
11	Исчерпано время жизни
12	Ошибка в параметре
13	Запрос временной метки
14	Ответ на запрос временной метки

Код

Однобайтовое поле, значение которого конкретизирует назначение ICMP-пакета определенного типа.

Например для **Тип 5** — Перенаправление

Характерны следующие коды:

Код 0 — Перенаправление пакетов в сеть
Код 1 — Перенаправление пакетов к узлу
Код 2 — Перенаправление для каждого типа обслуживания (TOS)
Код 3 — Перенаправление пакета к узлу для каждого типа обслуживания

Контрольная сумма

16-битовое поле, содержащее контрольную сумму, подсчитанную для всего ICMP-пакета целиком. Эта контрольная сумма вычисляется суммированием всех полей, начиная с поля Тип. При вычислении контрольной суммы значение поля **Контрольная сумма** полагается равным 0.

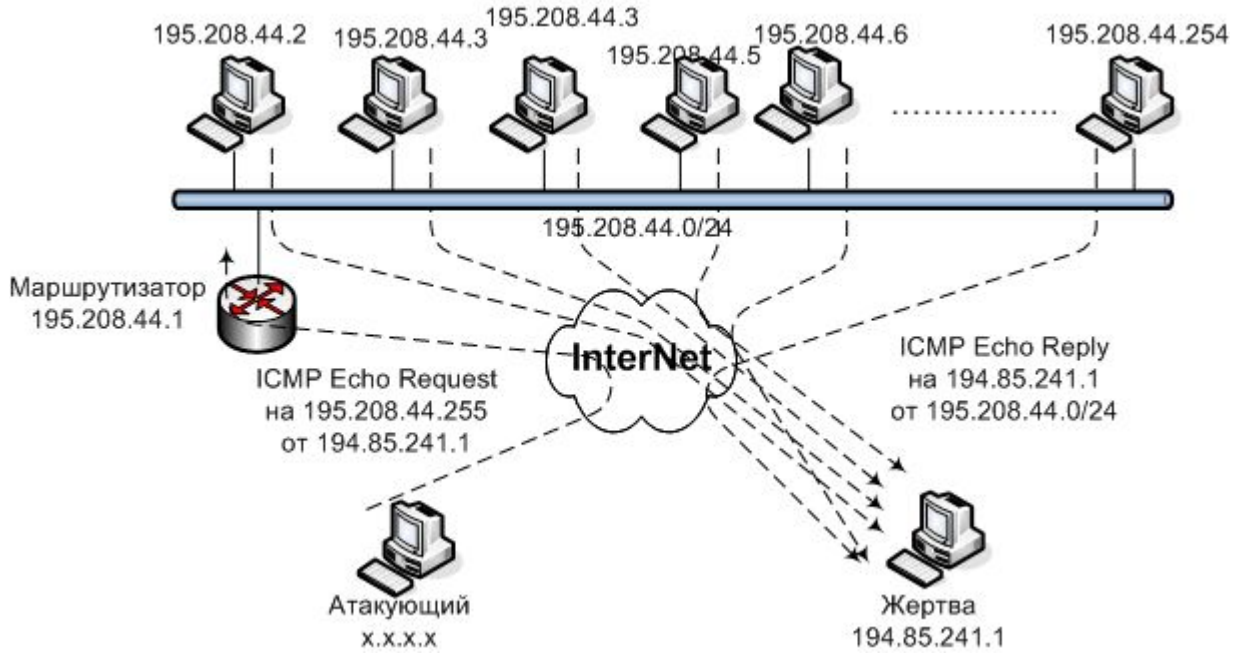
РАЗНОЕ

Четырехбайтовое поле, предназначенное для хранения разнообразной информации, специфичной для ICMP-пакетов определенного типа (например, номера в TCP-последовательности, IP-адреса и т.п.)

Тело пакета

Здесь содержится заголовок IP-пакета, явившегося причиной данного ICMP-пакета, и первые 8 байт данных тела этого IP-пакета. Если ICMP-пакет есть результат проявления аномалии в TCP- или UDP-взаимодействии, то эти 8 байт будут представлять собой первые восемь байтов, соответственно, TCP- или UDP-заголовка, что дает возможность определить, в частности, номера портов (а, следовательно, и использующие их прикладные программы). Для ICMP-пакетов некоторых типов **Тело пакета** может содержать не начало IP-пакета, а тестовые данные.

ICMP так же используется для проведения Атак.
Цель: загрузить сервер так, чтобы он не мог отвечать.
Нужно послать как можно больше ответов Echo Reply на «жертву».



Типы ICMP-пакетов

Рассмотрим 6 типов ICMP-пакетов, реализованных во всех клонах и версиях ОС UNIX.

Адресат недоступен

ICMP-пакет этого типа генерируется в следующих случаях:

- сеть, узел сети, протокол или порт являются недоступными;
- в ходе продвижения по сети IP-пакета потребовалась его фрагментация, однако в заголовке пакета установлен флаг DF, запрещающий делать это;
- предписываемый маршрут, указанный в поле дополнительных данных IP-пакета, оказался недействительным (несуществующим или неактивным).

Пример ICMP «Адресат недоступен» или «Tipe: 3». Параметр «Code: 1» указывает на недостижимость узла, к которому мы подключаемся.

No.	Time	Source	Destination	Protocol	Info
8239	13.999653	192.168.1.35	64.68.200.53	SMTP	C: HELO microsof459104
8240	14.001406	95.237.224.240	192.168.1.35	ICMP	Destination unreachable (Host unreachable)
8241	14.003452	192.168.1.35	192.234.69.31	IMF	from: "Enlarge with Promo" <engineun55@elsevier.com>, subject: COCKZI
8242	14.006095	192.168.1.35	93.100.1.3	DNS	Standard query MX yahoo.com.hk
8243	14.006767	66.212.12.14	192.168.1.35	SMTP	S: 220 aquahab.com ESMTP MDaemon 10.1.2; Wed, 29 Dec 2010 12:09:48 -(
8244	14.006785	206.183.112.45	192.168.1.35	SMTP	S: 220-osiris.accessmontana.com ESMTP

```
⊞ Frame 8240 (105 bytes on wire, 105 bytes captured)
⊞ Ethernet II, Src: ZyxelCom_8c:4c:25 (00:19:cb:8c:4c:25), Dst: Asiarock_f3:aa:cb (00:0b:6a:f3:aa:cb)
⊟ Internet Protocol, Src: 95.237.224.240 (95.237.224.240), Dst: 192.168.1.35 (192.168.1.35)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 91
    Identification: 0x61b1 (25009)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 48
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x2648 [correct]
    Source: 95.237.224.240 (95.237.224.240)
    Destination: 192.168.1.35 (192.168.1.35)
⊟ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 1 (Host unreachable)
    Checksum: 0xffe4 [correct]
```

Подавление источника

Механизм контроля потока данных гарантирует, что буфер приема не переполнится (V передачи < V приема).

Маршрутизаторы работают на уровне IP, и в их входящих очередях могут возникнуть пробки.

Пока идут ICMP-пакеты, передатчик снижает скорость.

При исчезновении ICMP-пакетов передатчик начинает увеличивать скорость.

Сообщение типа 4 имеет один код – 0.

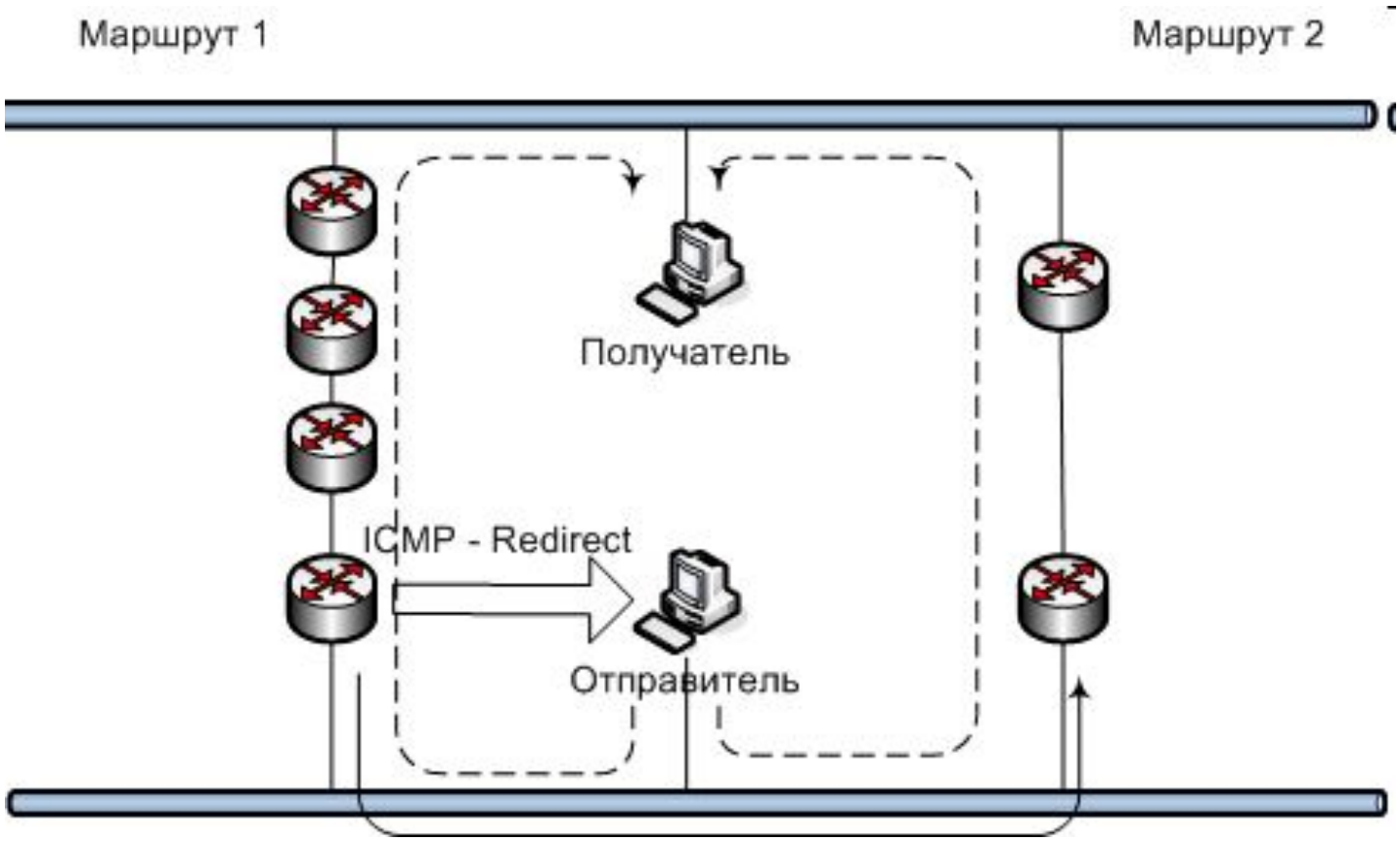
Перенаправление

Это сообщение посылается в том случае, когда маршрутизатор видит, что компьютер отправляет пакет некоторой сети назначения нерациональным образом, то есть не тому маршрутизатору сети, от которого начинается более короткий маршрут к сети назначения. Механизм перенаправления протокола ICMP позволяет компьютерам содержать в конфигурационном файле только IP-адреса его локальных маршрутизаторов.

Перенаправление *(продолжение)*

С помощью сообщений о перенаправлении маршрутизаторы будут сообщать компьютеру всю необходимую ему информацию о том, какому маршрутизатору следует отправлять пакеты для той или иной сети назначения. То есть маршрутизаторы передадут компьютеру нужную ему часть их таблиц маршрутизации.

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



ЭХО

Для реализации эха IP-модуль на узле **A** отправляет узлу **B** ICMP-пакет типа "запрос эха", содержащий в своем теле вместо IP-заголовка тестовые данные произвольной длины.

Узел **B**, получив такой запрос, возвращает узлу **A** ICMP-пакет типа "ответ на запрос эха", содержащий те же данные, что и в запросе.

ЭХО *(продолжение)*

Эхо-посылки используются для проверки достижимости удаленных узлов сети и измерения времени прохождения данных.

Исчерпано время жизни

ICMP-пакет данного типа посылается источнику IP-пакета, IP-пакет должен быть удален по одной из двух причин:

- исчерпано время жизни IP-пакета;
- исчерпано допустимое время на сборку фрагментированного IP-пакета.

Пример:

«Tipe: 11» превышение временного интервала

«Code: 0» время жизни пакета (TTL) истекло при транспортировке

No.	Time	Source	Destination	Protocol	Info
4503	8.243832	192.168.1.35	211.150.72.142	TCP	topflow > smtp [RST] Seq=85 Win=0 Len=0
4504	8.247265	219.141.134.25	192.168.1.35	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
4505	8.249500	192.168.1.35	65.54.188.72	TCP	geolocate > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4506	8.249537	192.168.1.35	208.87.233.190	TCP	personnel > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4507	8.250066	65.55.37.104	192.168.1.35	TCP	smtp > stss [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
4508	8.250084	192.168.1.35	65.55.37.104	TCP	stss > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0

```
⊞ Internet Protocol, Src: 219.141.134.25 (219.141.134.25), Dst: 192.168.1.35 (192.168.1.35)
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xbfa5 [correct]
  ⊟ Internet Protocol, Src: 192.168.1.35 (192.168.1.35), Dst: 211.150.72.142 (211.150.72.142)
      Version: 4
      Header length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      Total Length: 40
      Identification: 0xd1a5 (53669)
    ⊞ Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
    ⊞ Time to live: 1
      Protocol: TCP (0x06)
    ⊞ Header checksum: 0xca3a [correct]
      Source: 192.168.1.35 (192.168.1.35)
      Destination: 211.150.72.142 (211.150.72.142)
  ⊞ Transmission Control Protocol, Src Port: topflow (2885), Dst Port: smtp (25)
```

Неверный параметр

С помощью ICMP-пакета данного типа источник IP-пакета информируется о том, что данный пакет удален вследствие наличия ошибки в каком-либо из полей его заголовка.

Рассмотрим пример ICMP-пакета.

Filter: 192.168.1.33 Expression... Clear Apply

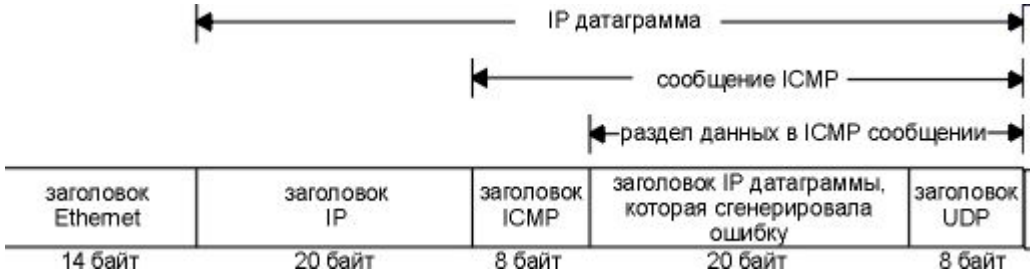
No.	Time	Source	Destination	Protocol	Info
374	116.546410	192.168.1.34	208.43.146.84	TCP	irdg-post > geognosisman [SYN]
375	116.628278	192.168.1.34	91.211.117.146	UDP	Source port: interintelli Dest
376	116.678027	91.211.117.146	192.168.1.34	ICMP	Destination unreachable (Port u
377	117.023176	192.168.1.34	192.168.1.255	NBNS	Name query NB ANWAERTERS.COM<00
378	117.773213	192.168.1.34	192.168.1.255	NBNS	Name query NB ANWAERTERS.COM<00

```
⊞ Ethernet II, Src: ZyxelCom_8c:4c:25 (00:19:cb:8c:4c:25), Dst: Asiarock_f3:aa:cb (00:0b:6a:f3:aa:cb)
⊞ Internet Protocol, Src: 91.211.117.146 (91.211.117.146), Dst: 192.168.1.34 (192.168.1.34)
⊟ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x904d [correct]
  ⊟ Internet Protocol, Src: 192.168.1.34 (192.168.1.34), Dst: 91.211.117.146 (91.211.117.146)
      Version: 4
      Header length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      Total Length: 35
      Identification: 0x5342 (21314)
    ⊞ Flags: 0x00
      Fragment offset: 0
      Time to live: 117
      Protocol: UDP (0x11)
    ⊞ Header checksum: 0x5f58 [correct]
      Source: 192.168.1.34 (192.168.1.34)
      Destination: 91.211.117.146 (91.211.117.146)
```

Рис.1

Перехват осуществлялся программой Wireshark. Домашняя локальная сеть анализировалась на предмет наличия ICMP-пакетов. Был обнаружен ICMP-пакет (рис. 1). Из содержания пакета видно, что при попытке подключения к хосту 91.211.117.146, мы получили ICMP-пакет с параметрами (Tipe: 3 Code: 3) .

Tipe: 3 – адресат недоступен

Code: 3 – порт недостижим

Из примера (рис. 1) следует, что UDP принимает датаграмму, порт назначения которой не соответствует порту, который обслуживается каким-либо процессом, UDP выдает ICMP-сообщение о недоступности порта. Вернувшееся ICMP-сообщение "порт UDP недоступен" будет иметь следующий вид: