UDP

NFS (Network File System), TFTP (Trivial File Transfer protocol, RFC-1350),
RPC (Remote Procedure Call, RFC-1057) и
SNMP (Simple Network Management Protocol, RFC-1157).

Хотя протокол UDP не гарантирует доставки, по умолчанию предполагается, что вероятность потери пакета достаточно мала.
UDP и в протоколе Teredo (туннелирование IPv6 для систем NAT)
На практике большинство систем работает с UDP-дейтограммами длиной 8192 байта

Новые порты UDP

- **Номер порта** **Обозначение** **Назначение**
- **1397** Audio-activmail Активная звуковая почта
- **1398** Video-activmail Активная видео-почта
- **6000-6063** X11 Система X Window

Стандартные номера портов UDP

Десятич. номер порта	Обозначение порта	Описание
20	FTP-data	
21	FTP	Протокол FTP
25	SMTP	
43	Whois	
80	WWW	
110	POP3	

Контрольное суммирование

ARP (Address Resolution Protocol)

RFC-**826**, **std-38**

Коды оборудования

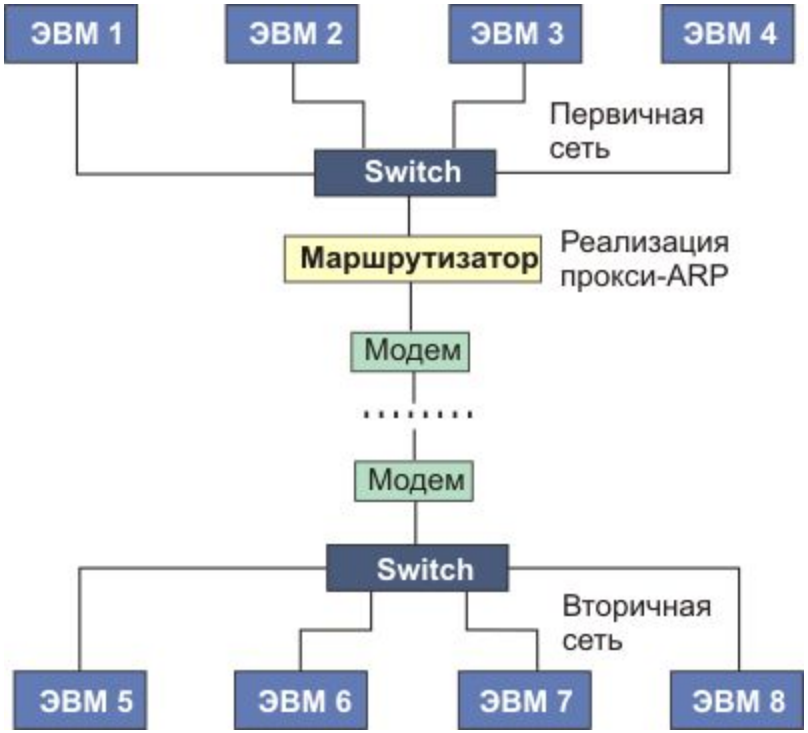
Код типа оборудования	Описание
1	Ethernet (10 Мбит/с)
3	X.25
4	Token Ring
6	IEEE 802

Коды протокола

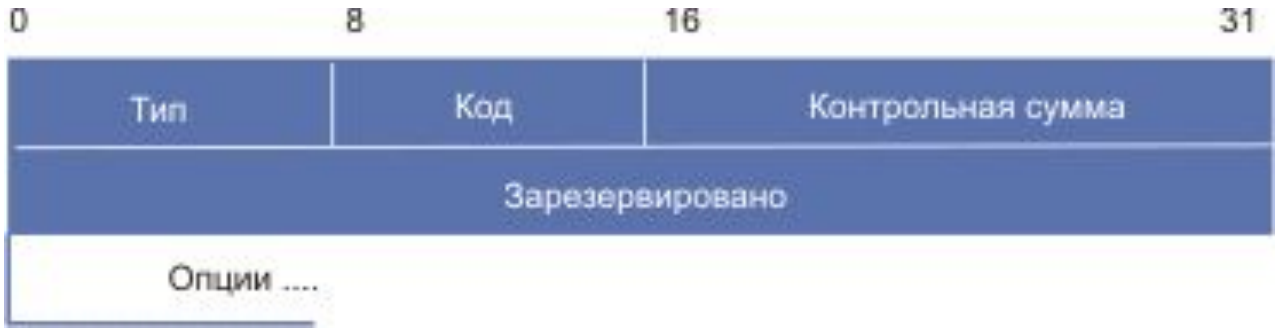
- 0806H ARP
- 0800H IP
- 814C SNMP

Возможны *самообращенные запросы* (**gratuitous ARP**). При таком запросе инициатор формирует пакет, где в качестве IP используется его собственный адрес. В таком запросе IP-адреса отправителя и получателя совпадают.
Определяется, нет ли в сети объекта, имеющего тот же IP-адрес. Если на такой запрос придет отклик, то ЭВМ выдаст на консоль сообщение Dublicate IP address sent from Ethernet address <...>.
В случае смены сетевой карты производится корректировка записи в ARP-таблицах ЭВМ, которые содержали старый MAC-адрес инициатора.

ARP-прокси


ЭВМ 1
ЭВМ 2
ЭВМ 3
ЭВМ 4
Первичная сеть
Switch
Маршрутизатор
Реализация прокси-ARP
Модем
Модем
Switch
Вторичная сеть
ЭВМ 5
ЭВМ 6
ЭВМ 7
ЭВМ 8

Формат сообщения запроса маршрутизатора (Neighbor Discovery - RFC-4861)



IP-поля (IP-заголовок пакета):

Адрес отправителя IP-адрес, приписанный отправляющему интерфейсу, или неспецифицированный адрес, если адрес отправляющему интерфейсу не присвоен.

Адрес получателя Обычно мультикаст адрес, соответствующий всем маршрутизаторам

Поля ICMP:

Тип=133

Код=0

ND (Neighbor Discovery - RFC-4861)

- *Выявление маршрутизатора:* алгоритм локализации маршрутизаторов, подключенных к каналу.
- *Определение префикса:* алгоритм детектирования списка адресных префиксов, которые определяют список объектов, подключенных к каналу. Узлы используют префиксы, чтобы разделить объекты, доступные непосредственно, от доступных через маршрутизатор.

- *Определение параметров:* механизм определения узлами параметров канала (такой как MTU канала) или параметры Интернет (такие как максимальное число шагов), которые вставляются в исходящие пакеты.
- *Автоконфигурация адреса:* определяет механизмы, необходимые для конфигурации адресов.
- *Выявление адреса:* задает алгоритм определения MAC-адреса соседа для заданного IP-адреса.
- *Определение следующего адреса:* маршрутизатор или само место назначения.
- *Детектирование недостижимости соседа:* Определяет механизм определения недостижимости соседа. Для соседей, используемых в качестве маршрутизаторов, может использоваться альтернативный маршрутизатор по-умолчанию. Как для соседей, так и для маршрутизатора

- *Детектирование адресов-дубликатов:* процедура определения узлом действителен ли используемый им адрес другого узла.
- *Перенаправление:* механизм информирования маршрутизатором машины о лучшем следующем шаге для конкретного места назначения.
- В протоколе ND определены пять разных типов ICMP-пакетов: два сообщения запроса и анонсирования маршрутизатора, два сообщения запроса и анонсирования соседа и сообщение переадресации

Формат сообщения анонсирования маршрутизатора

IP-поля (IP-заголовок пакета):

Адрес отправителя Должен быть локальным MAC-адресом, присвоенным интерфейсу, который посылает сообщение

Адрес получателя Обычно адрес отправителя вызывающего запрос маршрутизатора или мультикаст-адрес, соответствующий всем маршрутизаторам

Поля ICMP:

Тип=134

Код=0

Формат сообщения запроса соседа

IP поля (IP-заголовок пакета)

Адрес отправителя Либо адрес, приписанный интерфейсу, откуда пришло это сообщение

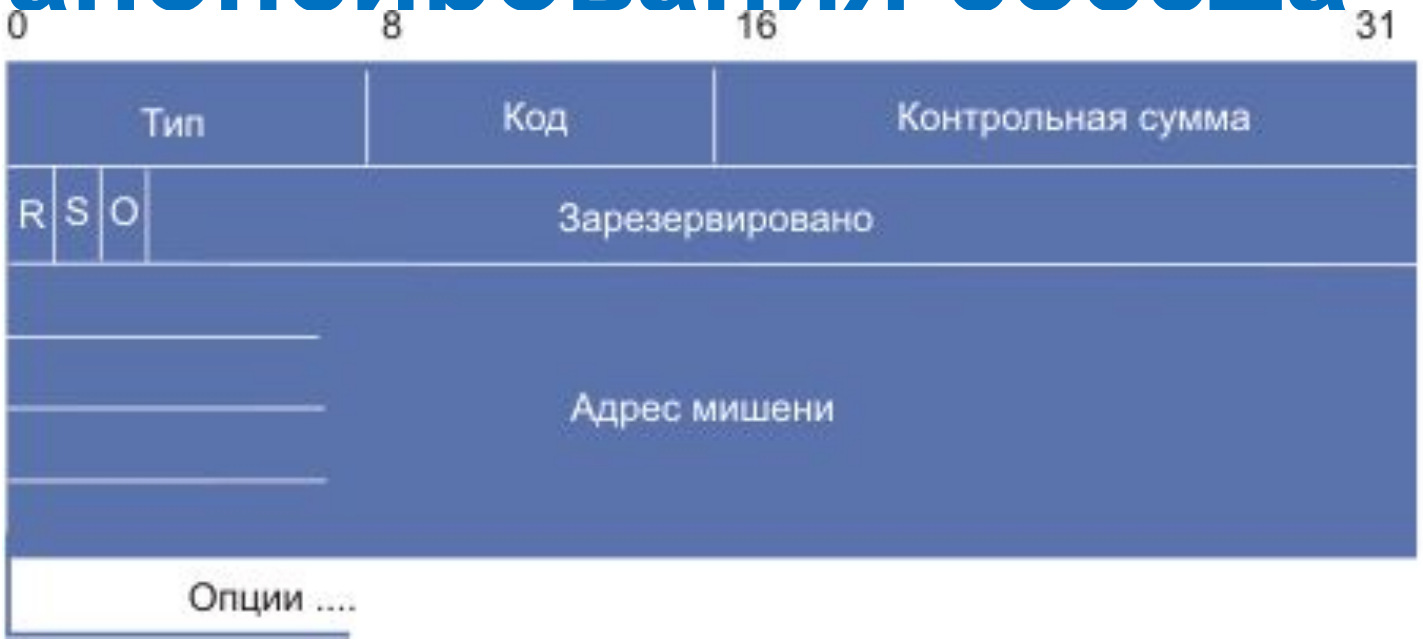
Адрес места назначения Либо мультикаст-адрес, соответствующий месту назначения, либо непосредственно адрес мишени

Поля ICMP:

Тип=135

Код=0

Формат сообщения анонсирования соседа



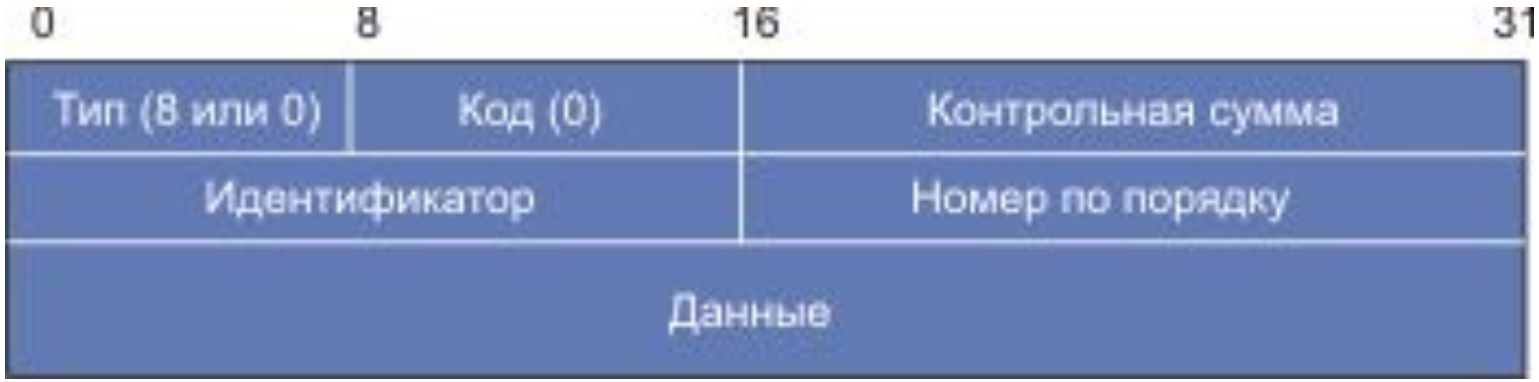
IP поля (IP-заголовок пакета)

Адрес отправителя Адрес присвоенный интерфейсу, через который послано сообщение анонсирования

Адрес места назначения Для запрошенных анонсирований адрес отправителя запроса или, если адресат запроса неспецифицирован, мультикаст-адрес всех узлов

- ***Поля ICMP (***Формат сообщения анонсирования соседа)***:***
  Тип=136
  Код=0
- ***R*** *- флаг маршрутизатора*. Если R=1, отправителем является маршрутизатор. R-бит используется при детектировании недостижимости соседа, чтобы детектировать маршрутизатор, который заменяет машину.
- ***S*** *- флаг запроса*. Когда S=1, это означает, что анонсирование было послано в ответ на запрос соседа со стороны адреса места назначения. S-бит используется в качестве подтверждения недоступности соседа. Бит не следует устанавливать в мультикастных уведомлениях или в случае неспровоцированного уникастного анонсирования.
- **O** - флаг перезаписи. Когда O=1, это означает, что анонсирование должно быть переписано существующей записью в кэше. Когда O=0, анонсирование не обновляет кэшированный MAC-адрес

ICMP (ping)



Поля ***идентификатор*** (обычно это идентификатор процесса) и ***номер по порядку*** (увеличивается на 1 при посылке каждого 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

Схема вложения ICMP-пакетов в Ethernet-кадр

Адресат не достижим

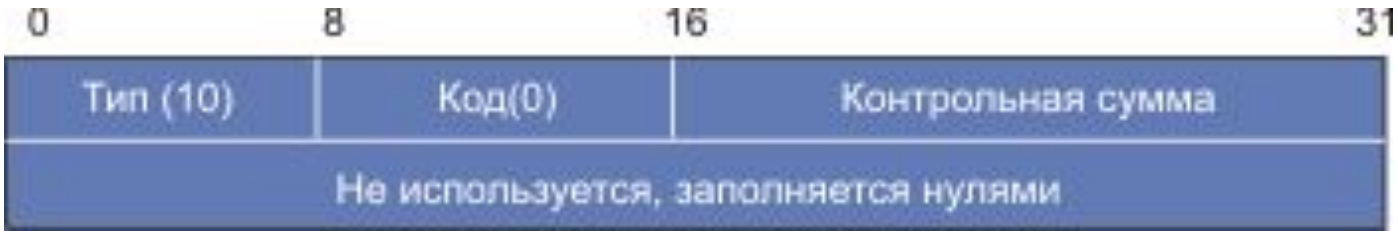
Quench


0
8
16
31
Тип (4)
Код(0)
Контрольная сумма
Не используется, заполняется нулями
Internet-заголовок (включая опции) + первые 64 байта дейтаграммы

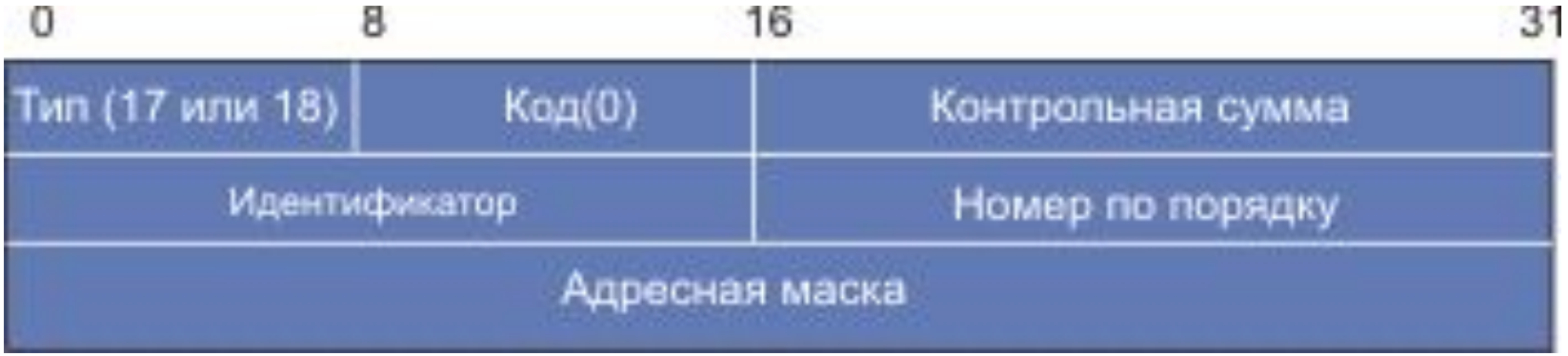
Формат ICMP-запроса переадресации

Формат ICMP-сообщений об имеющихся маршрутах

Формат запроса маршрутной информации

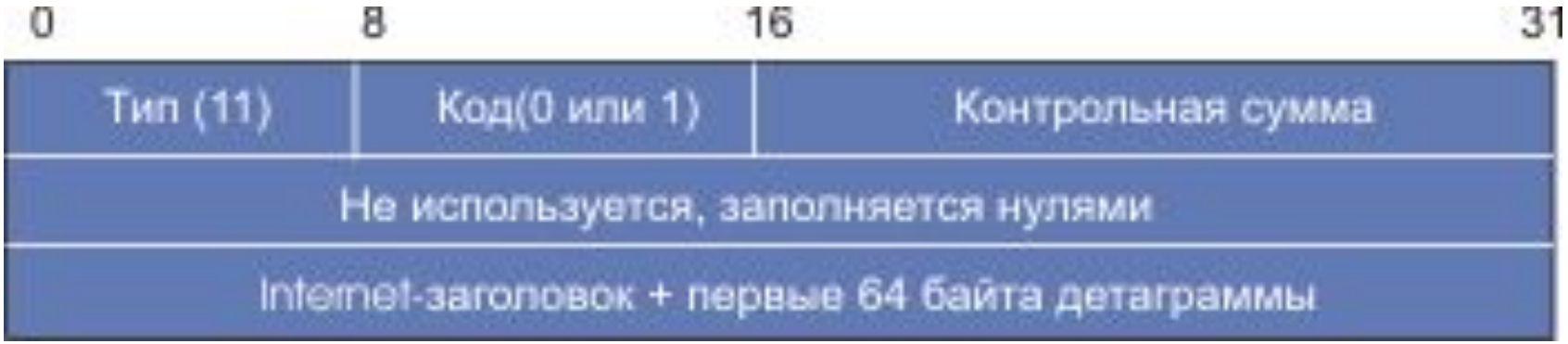


Формат запроса (отклика) маски субсети



тип=17 - это запрос, а тип=18 - отклик

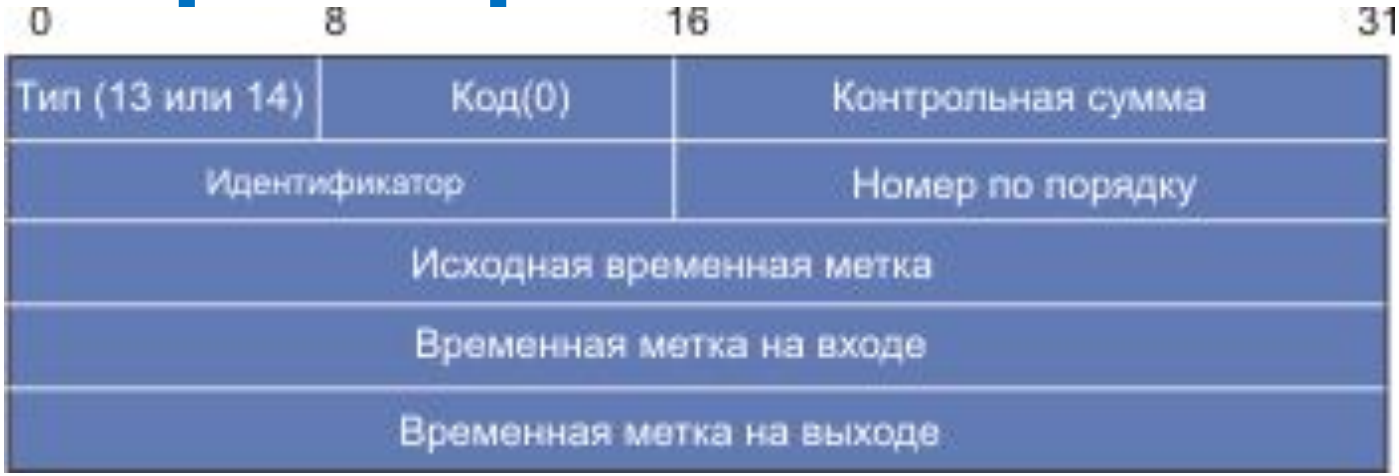
TTL=0



Код=0 *при передаче

Код=1 * при сборке (случай фрагментации).

Запрос временной метки



Поле *тип*=**13** указывает на то, что это запрос, а тип=**14** - на то, что это отклик

Поле ***идентификатор*** и ***номер по порядку*** используются отправителем для связи запроса и отклика. Поле ***исходная временная метка*** заполняется отправителем непосредственно перед отправкой пакета. Поле ***временная метка на входе*** заполняется маршрутизатором при получении этого пакета, а ***Временная метка на выходе*** -

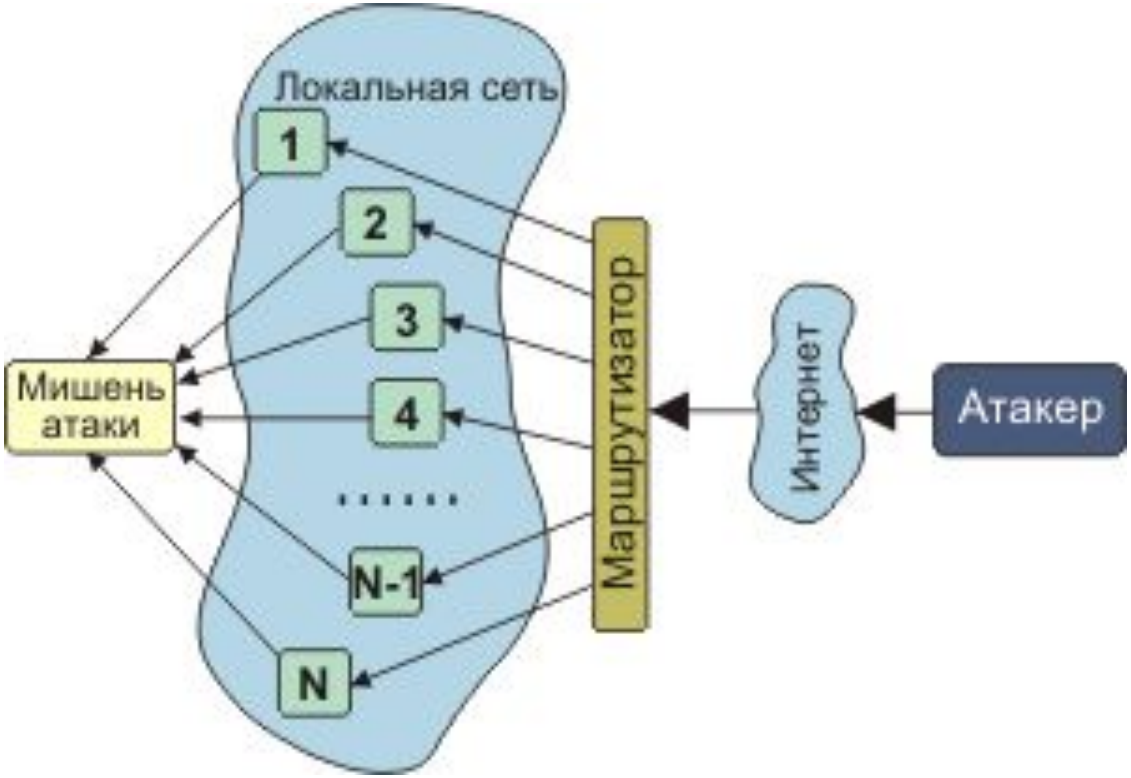
Конфликт параметров

Поле ***указатель*** отмечает октет дейтограммы, который создал проблему. ***Код***=1 используется для сообщения о том, что отсутствует требуемая опция (например, опция безопасности при конфиденциальных обменах), поле *указатель* при значении поля ***код***=1 не используется

ping -q mcmurdo-gw.mcmurdo.gov

- 193.124.224.190 ??? имя для GW ИТЭФ пока не придумано
- 193.124.137.13 MSU-Tower.Moscow.RU.Radio-MSU.net Вперед, в космос hop 3: 193.124.137.9 NPI-MSU.Moscow.RU.Radio-MSU.net Через спутник "Радуга"
- 193.124.137.6 DESY.Hamburg.DE.Radio-MSU.net пакеты совершили посадку в ДЕЗИ
- 188.1.133.56 dante.WiN-IP.DFN.DE
- 93.172.4.12 duesseldorf2.empb.net
- 193.172.4.8 amsterdam6.empb.net
- 193.172.12.6 Amsterdam1.dante.net Пересекаем Атлантический океан 194.41.0.42 New-York1.dante.net вступили на землю США
- 192.103.63.5 en-0.cnss35.New-York.t3.ans.net
- 140.222.32.222 mf-0.cnss32.New-York.t3.ans.net
- 140.222.56.2 t3-1.cnss56.Washington-DC.t3.ans.net
- 140.222.145.1 t3-0.enss145.t3.ans.net
- 192.203.229.243 SURA2.NSN.NASA.GOV Снова в космос
- 128.161.166.1 GSFC8.NSN.NASA.GOV но теперь через американский 128.161.232.1 GSFC12.NSN.NASA.GOV спутник <>
- 128.161.1.1 ARC1NEW.NSN.NASA.GOV
- 192.203.230.2 ARC1.NSN.NASA.GOV 192.100.12.2 ARC2.NSN.NASA.GOV

DDoS



К концу 2009 года предельные потоки DDoS-атак достигли 49 Гбит/с, а в 2014 – 200 Гбит/с!