



ICMR - ПРОТОКОЛ

ПРОТОКОЛ ICMP



ICMP (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений



Протокол IP предоставляет сервис передачи данных без гарантии доставки:



В случае ошибки при передаче пакета никаких действий не предпринимается



Функции ICMP:



1. Оповещение об ошибках на сетевом уровне



2. Тестирование работоспособности сети



Сообщения об ошибках ICMP не обязательно должны обрабатываться

ФОРМАТ ЗАГОЛОВКА ICMP

1 байт Тип сообщения	1 байт Код сообщения	2 байта Контрольная сумма
4 байта Служебная информация (зависит от типа и кода сообщения)		
Поле данных (фрагмент пакета, при передаче которого произошла ошибка)		

ТИПЫ ICMP- СООБЩЕНИЙ

Тип	Назначение сообщения
0	Эхо-ответ
3	Узел назначения недостижим
5	Перенаправления маршрута
8	Эхо-запрос
9	Сообщение о маршрутизаторе
10	Запрос сообщения о маршрутизаторе
11	Истечение времени жизни пакета
12	Проблемы с параметрами
13	Запрос отметки времени
14	Ответ отметки времени

*КОДЫ ICMP-
СООБЩЕНИЙ (ДЛЯ
ТИПА 3)*

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
5	Ошибка в маршруте источника
6	Сеть назначения неизвестна
7	Узел назначения неизвестен
8	Узел-источник изолирован
9	Административный запрет

ПРИМЕНЕНИЕ ICMP



Диагностика сети



Утилита ping



Утилита traceroute (в
Windows tracert)

УТИЛИТА PING

Проверка доступности компьютера в сети

Эхо-протокол ICMP:

- Эхо-запрос ICMP (Тип = 8, Код = 0)
- Эхо-ответ ICMP (Тип = 0, Код = 0)

УТИЛИТА PING



ICMP, Тип = 8, Код = 0



ICMP, Тип = 0, Код = 0

УТИЛИТА TRACEROUTE

tracertoute
определяет маршрут
от отправителя к
получателю

Находит адреса всех
маршрутизаторов,
через которые
проходит пакет

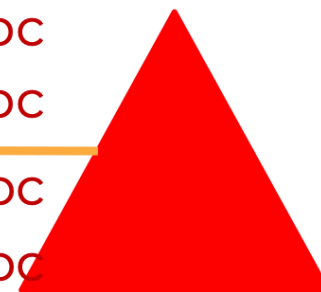
УГРОЗЫ СЕТЕВОГО УРОВНЯ

ICMP-флуд – отправка большого количества ICMP-пакетов с эхо-запросом

Злоумышленник



ICMP эхо-запрос
ICMP эхо-запрос
ICMP эхо-запрос
ICMP эхо-запрос
ICMP эхо-запрос
ICMP эхо-запрос
ICMP эхо-запрос





ИТОГИ

- ICMP (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений

Функции ICMP

- Оповещение об ошибках на сетевом уровне
- Тестирование работоспособности сети

Заголовок ICMP

- Тип сообщения
- Код сообщения

Утилиты, использующие ICMP

- ping
- traceroute