ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Сетевые протоколы передачи информации.
Протокол IP

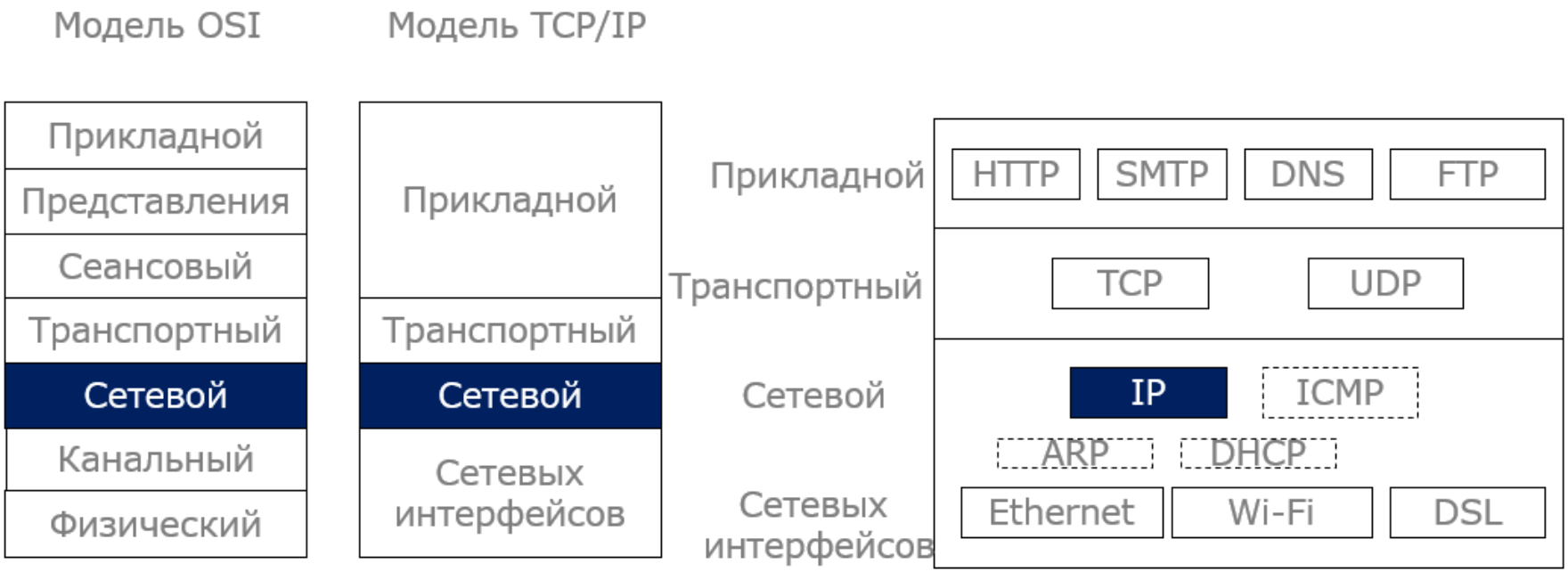
Место в моделях OSI и TCP/IP

Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO).

Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашел отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF).

- Модель OSI, которая была определена в серии стандартов ISO/IEC 7498, состоит из следующих частей:
- ISO/IEC 7498-1 — базовая модель;
- ISO/IEC 7498-2 — архитектура безопасности;
- ISO/IEC 7498-3 — наименования и адресация;
- ISO/IEC 7498-4 — система менеджмента.

Место в моделях OSI и TCP/IP



- Передача данных
  - без гарантии доставки
  - без сохранения порядка следования сообщений
- Протокол IP использует передачу данных без установки соединения

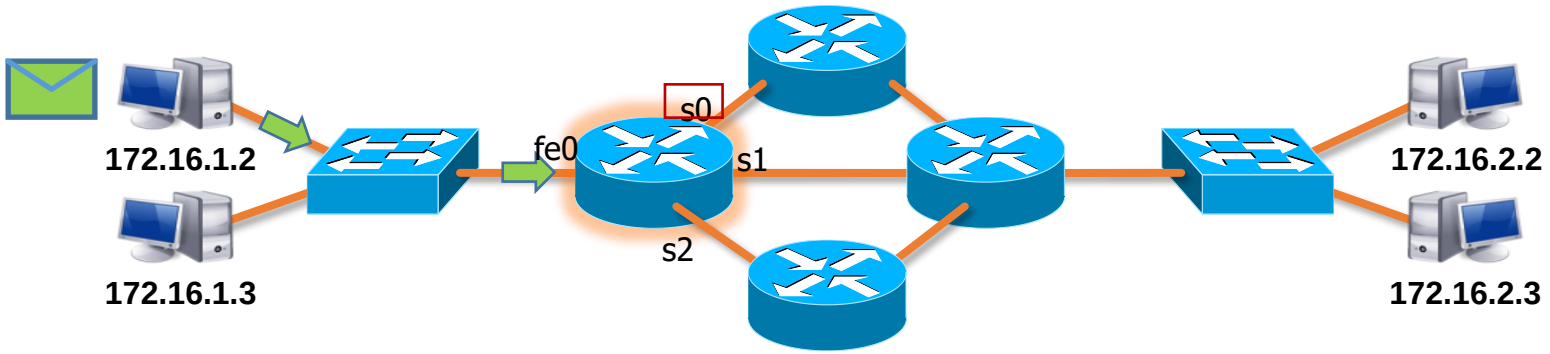
Задачи IP

- Объединение сетей
- Маршрутизация
- Качество обслуживания

Коммутация каналов/пакетов

- Коммутация - экономичное продвижение пакетов на основании локального адреса Обеспечивается продвижение пакета между «соседями»:
  - одной локальной сети (не разделенной маршрутизаторами)
  - по каналу «точка-точка» глобальной сети

1. Таблицы коммутации небольшого размера – учитываются только адреса активно взаимодействующих «соседей»
2. Пакет при продвижении не модифицируется – экономия действий, стоимость скорости



Формат заголовка IP-пакета

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина
16 бит Идентификатор пакета		3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни	8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя			
32 бита IP-адрес получателя			
Опции и выравнивание (не обязательно)			

Тип протокола (код протокола, данные которого передаются):

TCP – 6
UDP – 17
ICMP – 1

Заголовок IP-пакета может включать дополнительные поля:

- Записать маршрут
- Маршрут отправителя
  - Жёсткая маршрутизация
  - Свободная маршрутизация
- Временные метки

Общая длина – длина пакета, включая заголовок и данные (измеряется в байтах, максимальное значение – 65535 байт, выбирается с учетом размера кадра канального уровня 1500 байт для Ethernet)

Время жизни (TTL, Time To Live) – максимальное время, в течение которого пакет может перемещаться по сети (введено для предотвращения «бесконечного» продвижения пакетов, секунды, прохождение через маршрутизатор (hop)
Предназначено для реализации функции мультиплексирования/ демультиплексирования

Заполнение:

- Опции могут иметь разный размер
- Длина заголовка IP-пакета должна быть кратна 32 битам
- Для выравнивания до 32 бит поле опций дополняется нулями

Формат заголовка IP-пакета

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина	
16 бит Идентификатор пакета			3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни		8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя				
32 бита IP-адрес получателя				
Опции и выравнивание (не обязательно)				

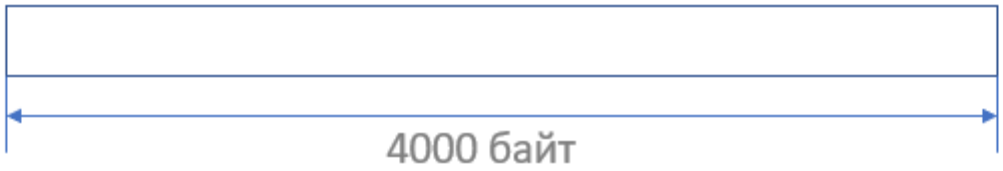
Пример

- Исходный пакет 4000 байт (заголовок 20 байт, данные 3980 байт)
- MTU целевой сети 1500 байт (заголовок 20 байт, данные 1480 байт,)
- Три фрагмента данные: 0-1479, 1480-2959, 2960-3980, равные заголовок +сами данные=1500)
- Смещение фрагментов: 0, 185, 370 (проверяем: необходимо получить начало поля данных во втором сегменте = 1480/8=185
- В третьем блоке =2960/8=370

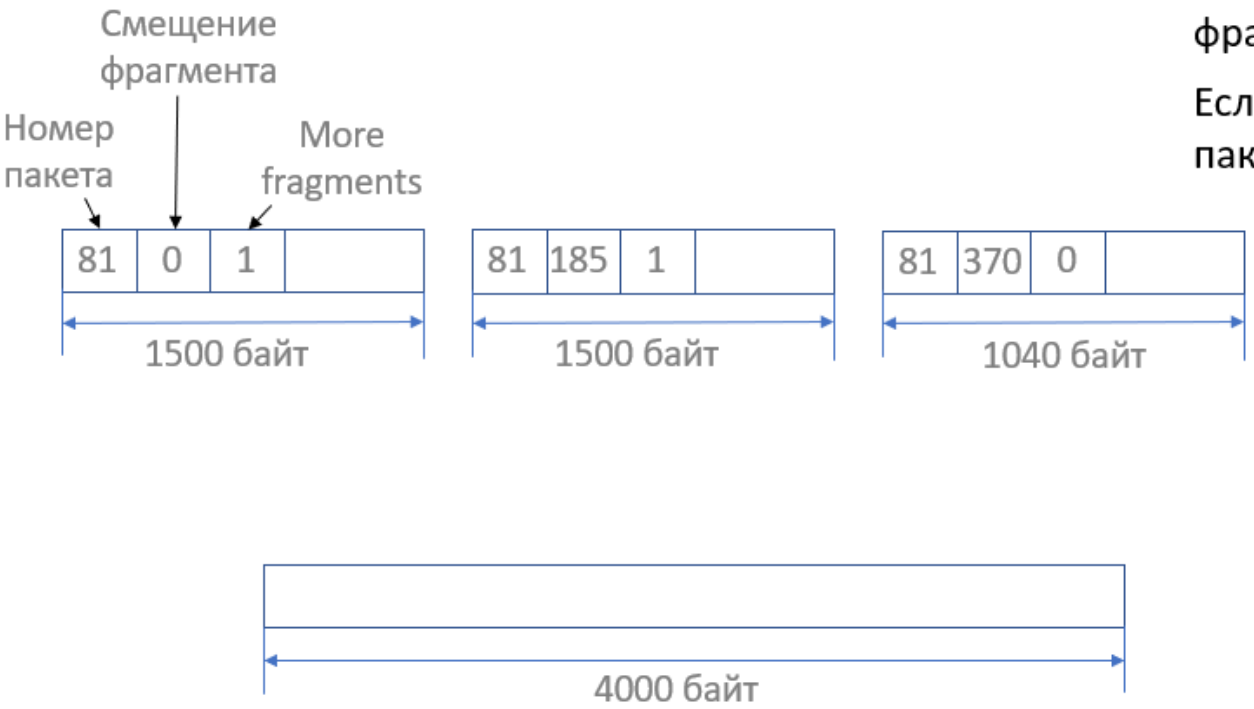
- Протокол IP работает на сетевом уровне
  - Объединение сетей, построенных на основе разных технологий
- Различия в сетях
  - Максимальный размер передаваемых данных (Maximum Transmission Unit, MTU)
  - Ethernet – 1500 байт
  - Token Ring – 4464 байта
  - FDDI – 4352 байта
- Фрагментация – разделение пакета на несколько частей (**фрагментов**) для передачи по сети с маленьким MTU
- Размер поля флаги – 3 бита
- Значения полей
  - Первый бит зарезервирован и не используется
  - DF (Don't Fragment) – не фрагментировать
  - MF (More Fragments) – есть еще фрагменты
- **Смещение фрагмента** в поле данных исходного пакета
  - Измеряется в 8-байтовых блоках
  - Определяет позицию фрагмента в потоке данных

Нарушение безопасности:
неправильная фрагментация-неправильная сборка-нарушение работоспособности

Фрагментация IP-пакета



Сборка IP-пакета



Обеспечение безопасности

Флаг DF (Don’t Fragment) запрещает фрагментацию пакета

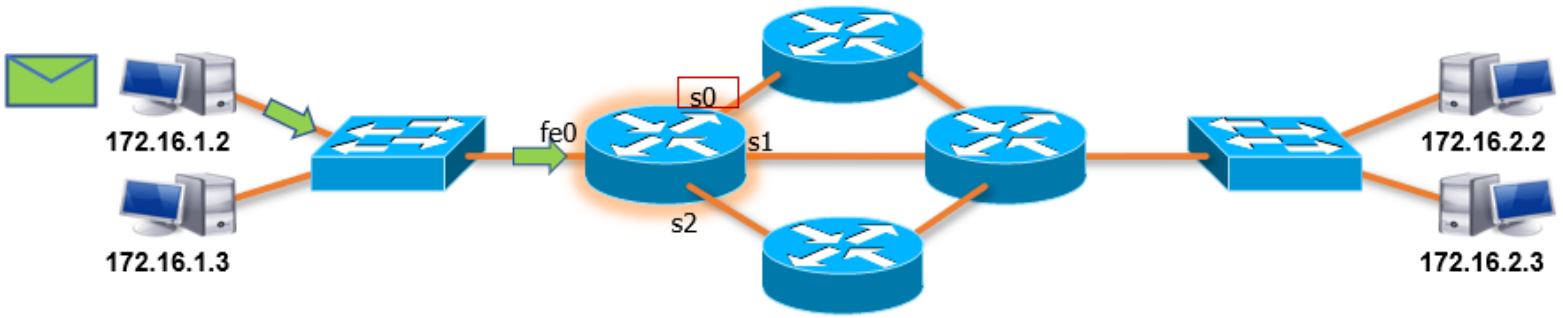
Если MTU сети меньше размера пакета

- Маршрутизатор отбрасывает пакет
- Получателю отправляется ICMP сообщение Тип 3, Код 4 (Destination Unreachable, Fragmentation required, and DF flag set)
- Проблема блокирование пакетов ICMP

Протокол IP. Безопасность

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина	
16 бит Идентификатор пакета			3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни		8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя				
32 бита IP-адрес получателя				
Опции и выравнивание (не обязательно)				

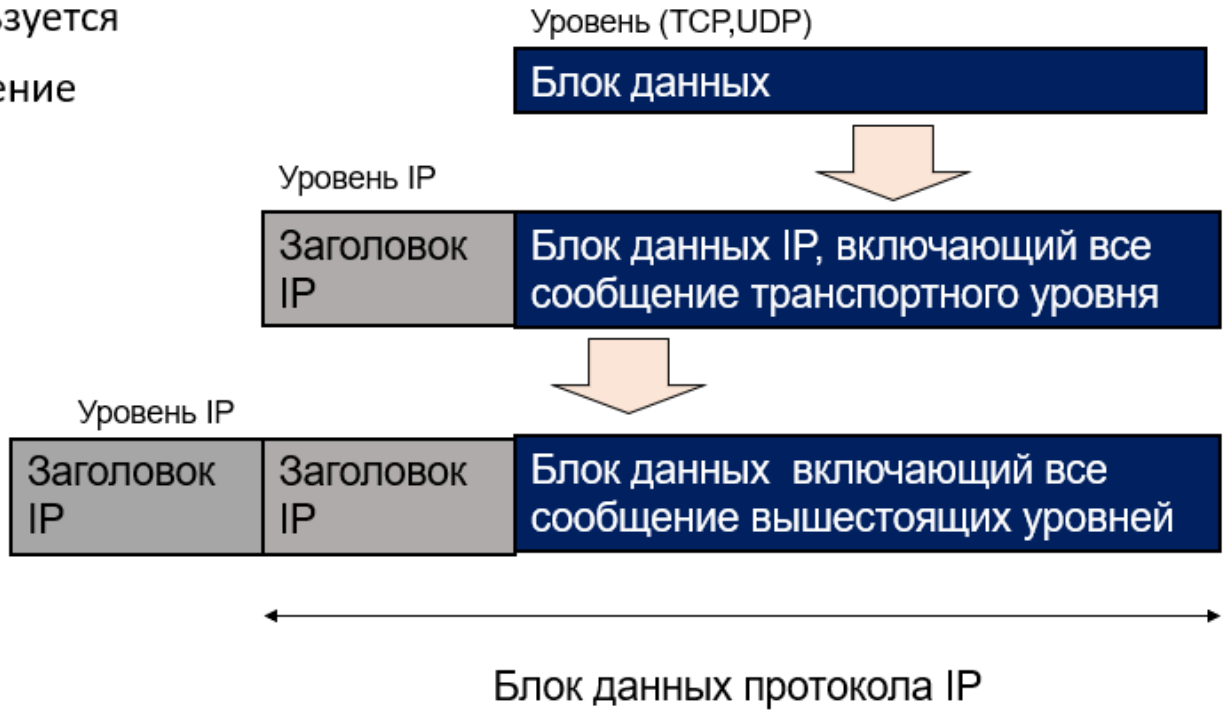
- Идентификатор пакета- неправильное указание идентификатора создает нарушение при сборке пакета
- Флаги- установка флага на запрет фрагментации – нарушения безопасности при передаче между сетями
- Смещение фрагмента- неправильное указание смещения создает нарушение при сборке пакета
- Контрольная сумма- повторная передача и уменьшение пропускной способности сети
- IP адреса- подмена IP адреса



Протокол IP. Туннелирование

Туннелирование используется при необходимости

- Сокрытия в сети IP адресов.
- Данный механизм используется
- В том числе и для построение
- VPN



Инкапсуляция протоколов

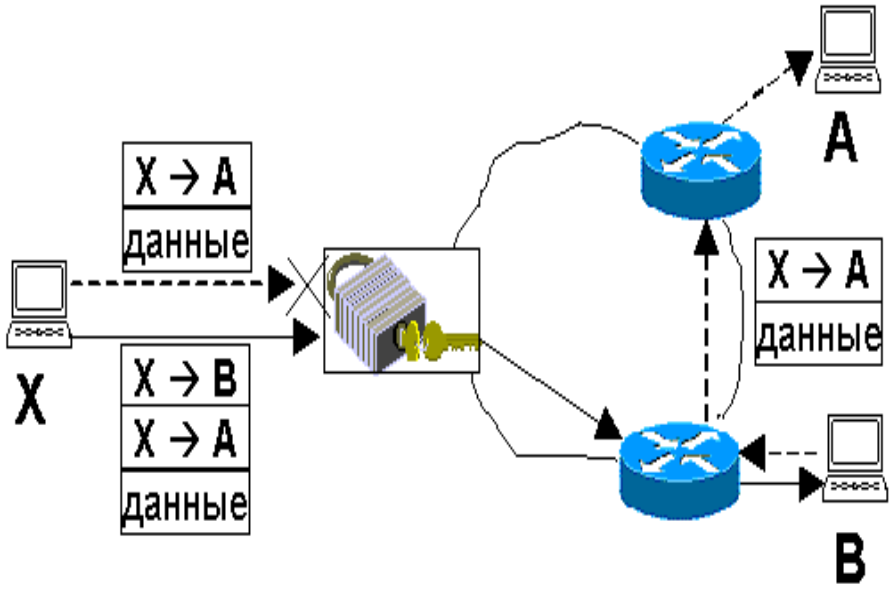
Правила фильтрации запрещают отправку дейтограмм узлу А узлом Х, но разрешают узлу В. Для осуществления атаки злоумышленник:

формирует дейтограмму, заголовок которой заполняет стандартным способом.

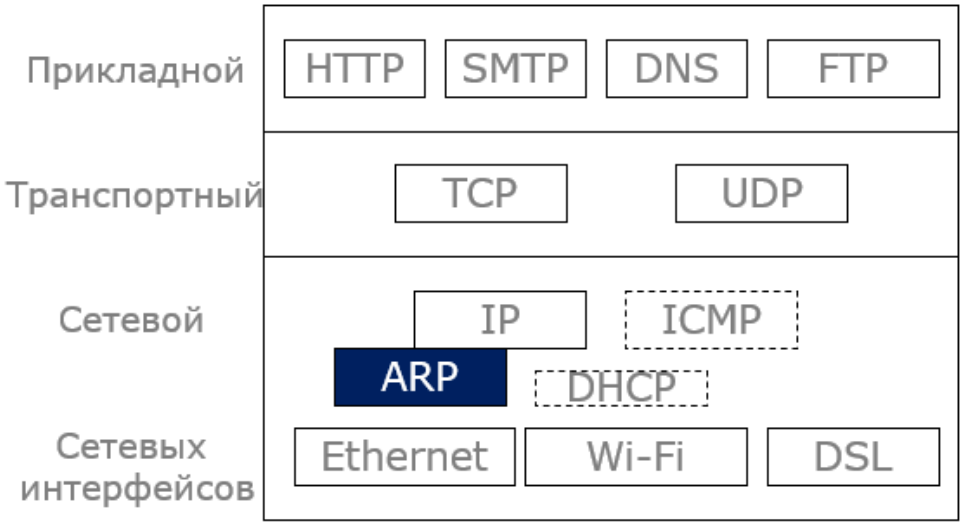
Данная дейтограмма инкапсулируется в новую IP-дейтограмму, при этом в поле протокола указывается, инкапсуляция и адрес промежуточного узла В.

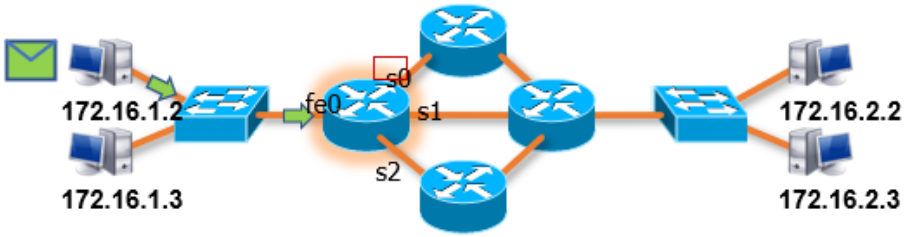
Получив данную дейтограмму узел В анализирует первый заголовок видит, что дейтограмма адресована не узлу А и отправляет ее по назначению, снабдив новым заголовком

В данном случае фильтрующий узел видит, что дейтограмма пришла с разрешенного узла и пропускает ее.



Протокол ARP





- ARP (Address Resolution Protocol) – протокол разрешения адресов
- Данные передаются с помощью технологии канального уровня:
  - Ethernet, Wi-Fi, MAC-адреса
- Протокол ARP позволяет автоматически определить MAC-адрес компьютера по его IP-адресу
- ARP работает в режиме запрос-ответ

Таблица соответствия

```
$ cat /etc/ethers
00:17:31:A7:83:34 192.168.1.2
00:17:31:A7:83:0C 192.168.1.3
00:17:31:2E:3C:EE 192.168.1.4
00:17:31:A7:83:48 192.168.1.5
00:17:31:A7:83:68 192.168.1.6
00:17:31:9A:ED:A5 192.168.1.7
00:17:31:A7:84:3A 192.168.1.8
00:17:31:A7:83:5A 192.168.1.9
00:17:31:A7:83:F8 192.168.1.10
```

Протокол ARP

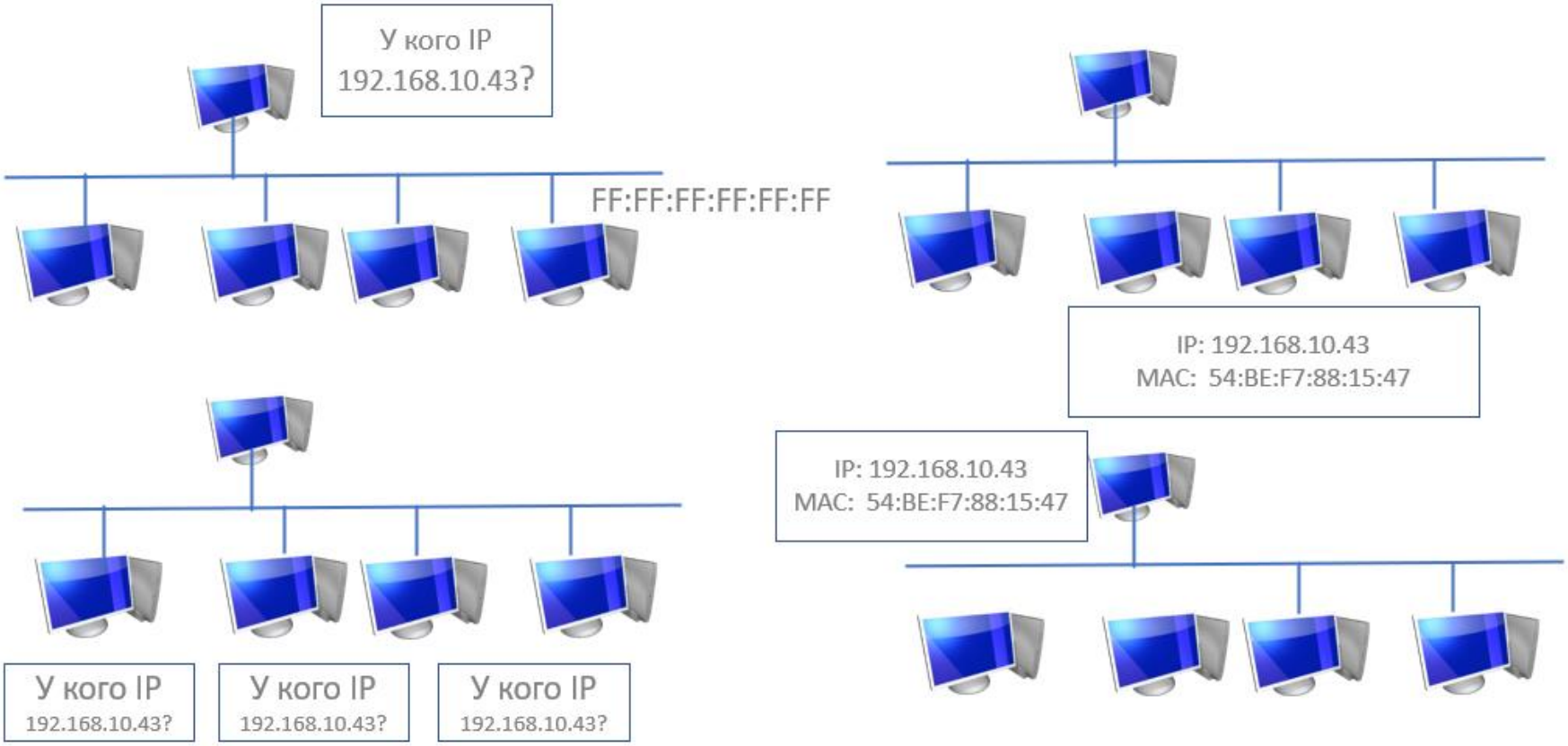
Поле	Значение
Тип сети	1
Тип протокола	2048
Длина локального адреса	6
Длина глобального адреса	4
Операция	1
Локальный адрес отправителя	1C:75:08:D2:49:45
Глобальный адрес отправителя	192.168.10.15
Локальный адрес получателя	00:00:00:00:00:00
Глобальный адрес получателя	192.168.10.43

Режим работы запрос-ответ:

- Запрос отправляется на широковещательный адрес
- Ответ посылает только компьютер с запрошенным IP-адресом

Результаты работы протокола ARP записываются в ARP-таблицу на компьютере

ARP-запрос


У кого IP
192.168.10.43?
FF:FF:FF:FF:FF:FF
IP: 192.168.10.43
MAC: 54:BE:F7:88:15:47
IP: 192.168.10.43
MAC: 54:BE:F7:88:15:47
У кого IP
192.168.10.43?
У кого IP
192.168.10.43?
У кого IP
192.168.10.43?

ARP-запрос

Поле	Значение
Тип сети	1
Тип протокола	2048
Длина локального адреса	6
Длина глобального адреса	4
Операция	2
Локальный адрес отправителя	54:BE:F7:88:15:47
Глобальный адрес отправителя	192.168.10.43
Локальный адрес получателя	54:BE:F7:88:15:47
Глобальный адрес получателя	192.168.10.15

```
C:\Users\User>arp -a

Интерфейс: 192.168.1.226 --- 0xc
  адрес в Интернете      Физический адрес      Тип
  192.168.1.1           70-4d-7b-4d-63-14     динамический
  192.168.1.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  255.255.255.255       ff-ff-ff-ff-ff-ff     статический
```

ARP пакеты не проходит через маршрутизаторы

Для отправки и получения пакетов данных маршрутизаторы строят собственные ARP-таблицы, в которых отображаются IP-адреса на MAC-адреса.

Маршрутизатор может быть подключен к нескольким подсетям и строит ARP-таблицы, описывающие все сети, подключенные к нему.

Кроме карт соответствия IP-адресов MAC-адресам в таблицах маршрутизаторов отображаются порты.

Для осуществления маршрутизации в сетях IP, маршрутизаторы содержат MAC- и IP-адреса других маршрутизаторов, которые используются для перенаправления пакетов.

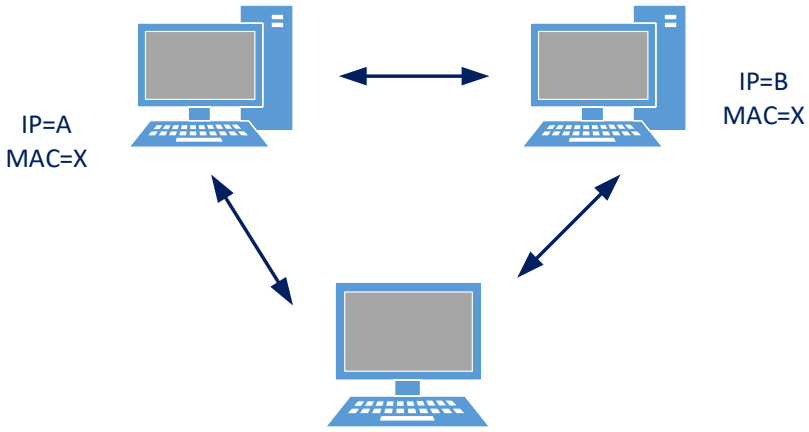
Протокол ARP

Ложные ARP-ответы

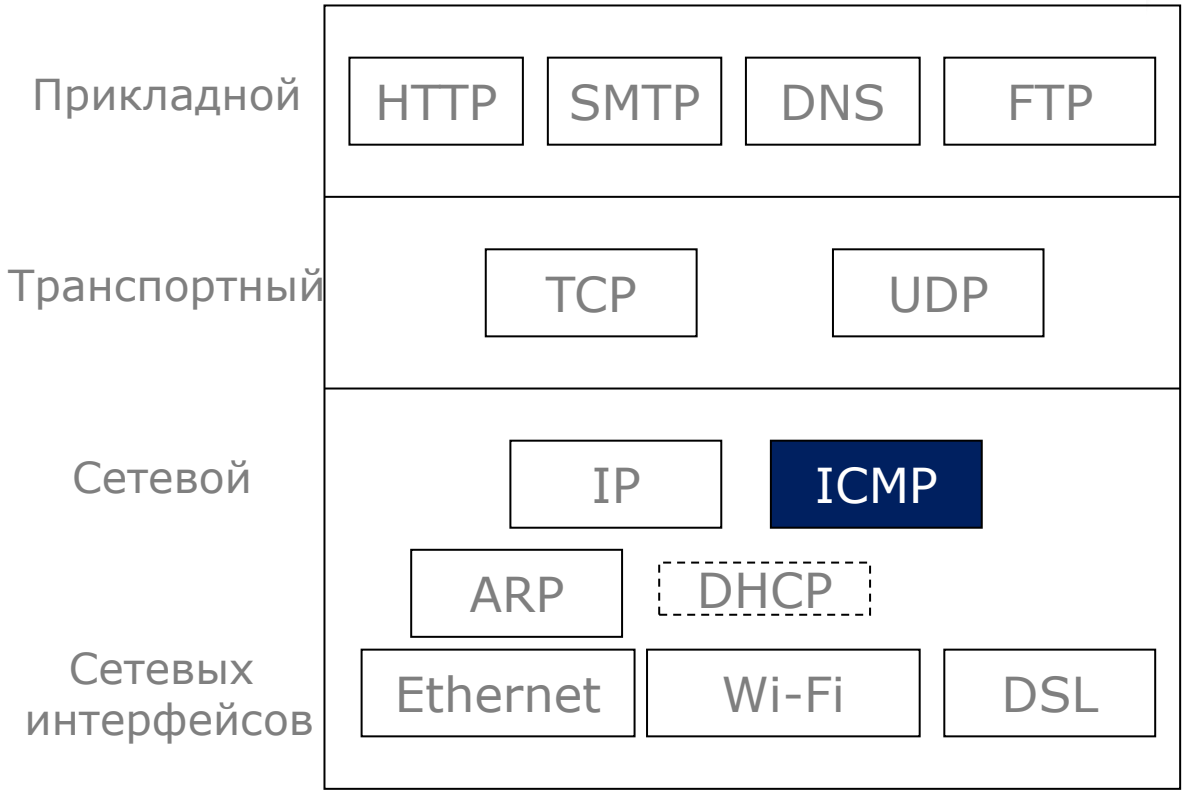
Злоумышленник X определяет MAC адреса узлов A и B.

На компьютере X конфигурируется логические IP интерфейсы, с именами адресов A и B. Устанавливается статическая ARP-таблица и разрешается ретрансляция дейтаграмм.

На MAC-адреса узла A отправляется сфабрикованный ARP-ответ, в котором сообщается, что IP-адресу B соответствует MAC –адрес X. Аналогичный ответ отправляется узлу B. В связи с тем, что ARP-протокол без сохранения состояния, то узлы A и B примут ARP-ответ, даже если они не посылали запрос.



Протокол ICMP



Протокол ICMP

IP предоставляет сервис передачи данных без гарантии доставки:

- В случае ошибки при передаче пакета никаких действий не предпринимается

- Функции ICMP
  - Оповещение об ошибках на сетевом уровне
  - Тестирование работоспособности сети

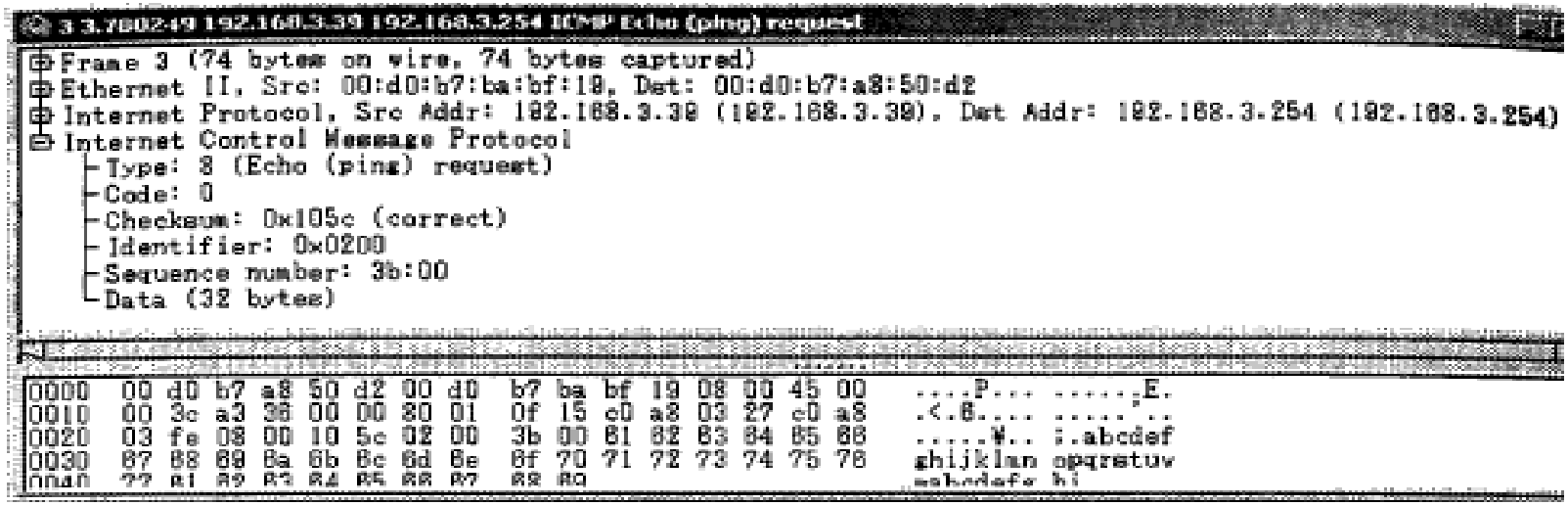
Сообщения об ошибках ICMP не обязательно должны обрабатываться

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

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

- Не требует номера портов для работы
- Не посылает сообщение об ошибке в ответ на полученное, тем самым не загружая сеть
- Для фрагментированных дейтограмм сообщение протокола посылается только для первого фрагмента ICMP (сообщение об ошибке и запрос для определения характеристик сети)
- Сообщение имеет вид



Применение ICMP

- Диагностика сети
- Утилиты
  - ping
  - traceroute (в Windows tracert)

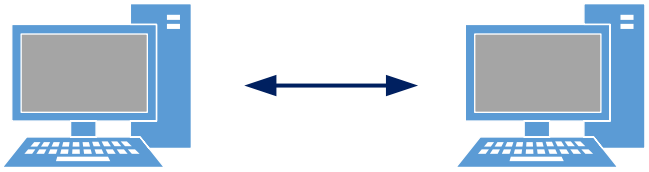
- С помощью отправки сообщений с эхо-запросом по протоколу ICMP проверяет соединение на уровне протокола IP с другим компьютером, поддерживающим TCP/IP. После каждой передачи выводится соответствующее сообщение с эхо-ответом.

- **Синтаксис команды**
  - **ping** [**-t**] [**-a**] [**-n** *счетчик*] [**-l** *размер*] [**-f**] [**-i** *TTL*] [**-v** *тип*] [**-r** *счетчик*] [**-s** *счетчик*] [{**-j** *список_узлов* | **-k** *список_узлов*}] [**-w** *интервал*] [*имя_конечного_компьютера*]

  - **tracert [-d]** [-h *максимальное_число_переходов*] [-j *список_узлов*] [-w *интервал*] [*имя_конечного_компьютера*]

Утилита ping

- **Особенности работы:**
- Проверка доступности компьютера в сети
- Эхо-протокол ICMP:
  - Эхо-запрос ICMP (Тип = 8, Код = 0)
  - Эхо-ответ ICMP (Тип = 0, Код = 0)



ICMP, Тип = 8, Код = 0 ICMP, Тип = 0, Код = 0

```
C:\Users\User>ping vk.com

Обмен пакетами с vk.com [87.240.190.67] с 32 байтами данных:
Ответ от 87.240.190.67: число байт=32 время=5мс TTL=58
Ответ от 87.240.190.67: число байт=32 время=2мс TTL=58
Ответ от 87.240.190.67: число байт=32 время=5мс TTL=58
Ответ от 87.240.190.67: число байт=32 время=2мс TTL=58

Статистика Ping для 87.240.190.67:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 5 мсек, Среднее = 3 мсек
```

ping vk.com
Обмен пакетами с vk.com [87.240.131.120] с 32 байтами данных:
Ответ от 87.240.131.120: число байт=32 время=42мс TTL=49
Ответ от 87.240.131.120: число байт=32 время=41мс TTL=49
Ответ от 87.240.131.120: число байт=32 время=41мс TTL=49
Ответ от 87.240.131.120: число байт=32 время=42мс TTL=49
Статистика Ping для 87.240.131.120:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 41мсек, Максимальное = 42 мсек, Среднее = 41 мсек

Безопасность ICMP

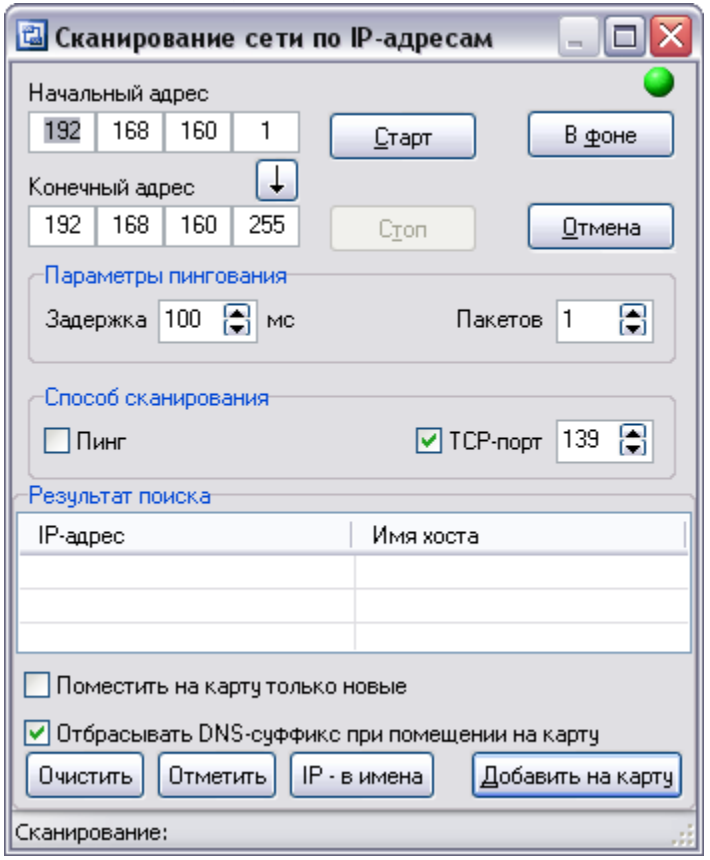
- **Особенности работы:**

1.Сканирование подключенных к сети компьютеров осуществляется с помощью программы ping посылкой ICMP-сообщений Echo по широковещательному адресу, на которое ответят все компьютеры, поддерживающие обработку данных сообщений

2. Сканирование портов (см TCP)

3. Поиск уязвимостей в ОС

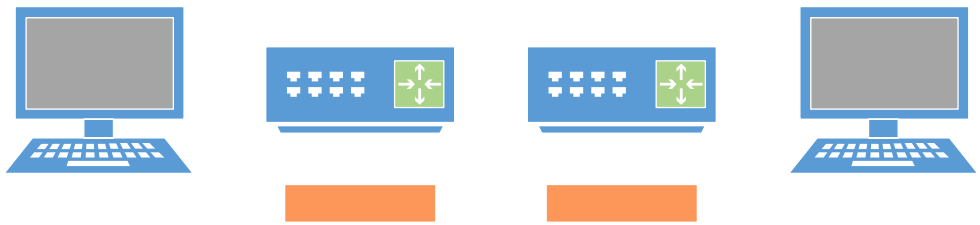
4. Подбор паролей



Утилита traceroute

Особенности работы:

- traceroute определяет маршрут от отправителя к получателю
- Находит адреса всех маршрутизаторов, через которые проходит пакет



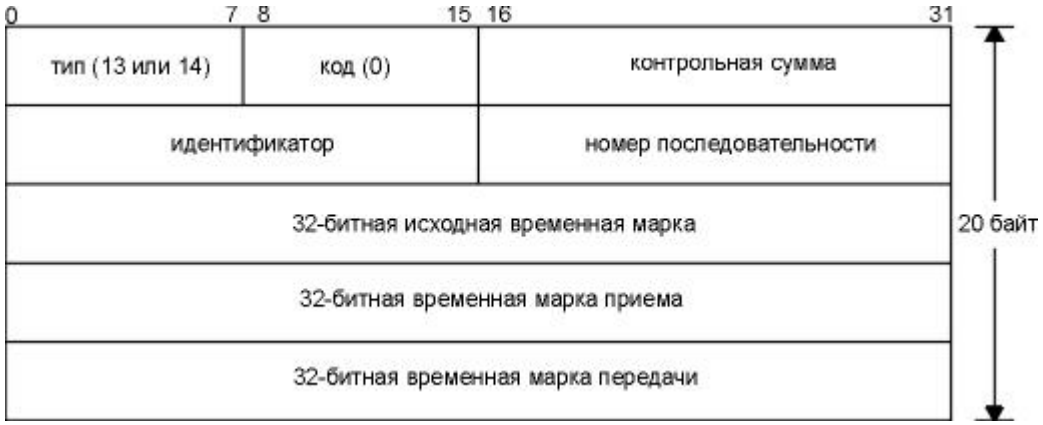

```
  2     3 ms    16 ms     2 ms  5x19x0x194.static-business.spb.ertelecom.ru [5.1
9.0.194]
  3    39 ms    31 ms     6 ms  5x19x0x225.static-business.spb.ertelecom.ru [5.1
9.0.225]
  4     3 ms     2 ms     3 ms  lag-0-160.bbr01.spb.ertelecom.ru [188.234.131.23
3]
  5     3 ms     3 ms     7 ms  net131.234.188-124.ertelecom.ru [188.234.131.124
]
  6     *        *        *     Превышен интервал ожидания для запроса.
  7     *        *        *     Превышен интервал ожидания для запроса.
  8     3 ms     3 ms     3 ms  93.186.225.208

Трассировка завершена.
```

Трассировка маршрута к vk.com [87.240.131.120]
с максимальным числом прыжков 30:

1 3 ms 1 ms 1 ms 10.113.192.62
2 1 ms 1 ms 1 ms 10.255.34.10
3 101 ms 1 ms 10 ms 10.255.34.4
4 4 ms 1 ms 1 ms 10.255.31.1
5 1 ms 4 ms 1 ms 10.255.31.9
6 1 ms 1 ms 1 ms 10.96.242.1
7 41 ms 41 ms 42 ms srv120-131-240-87.vk.com [87.240.131.120]

Трассировка завершена.

Безопасность ICMP



- **Информационные запросы:**
- icmp timestamp request (type 13, 14)- запрос временной метки позволяет системе запросить другую систему о текущем времени. Рекомендуемое значение, которое должно быть возвращено, это количество миллисекунд, которые прошли с полуночи в формате UTC, (Универсальное согласованное время - Coordinated Universal Time). Формат ICMP запроса и формат ICMP отклика временной марки.
- ***Возможная атака:*** сканирование сети, путем посылки запросов с временной метки, ответ на которую будет сообщением о том, что хост подключен к сети.
- **ICMP parameter problem**
- Сообщение если маршрутизатор или хост при извлечении заголовка испытывает сложности в интерпретации полей заголовка.
- С использованием данного сообщения атакующий может получить информацию о сканируемом хосте, производителе, открытых портах. Для этого формируется сообщение с некорректно сформированным заголовком, но с правильно указанным портом и инкапсуляцией в пакет TCP. При получении ответа на данное сообщение можно оценить о наличии узла, об открытии порта

Безопасность ICMP

Destination Unreachable (Адресат недоступен). Отправляется маршрутизатором при невозможности доставки дейтограммы в случаях когда:

- возникает необходимость фрагментации дейтограммы, а флаг DF запрещает фрагментацию;
- у маршрутизатора нет маршрута в сеть назначения дейтограммы;
- указанный в дейтограмме протокол вышестоящего уровня не поддерживается получателем;
- правила фильтрации запрещают передачу пакета к месту назначения.
- ***Атака***: Данные сообщения могут использоваться для нарушения связи между отправителем и получателем, путем отправки сообщения Destination Unreachable со стороны злоумышленника (например, для разрыва связи между хостами).

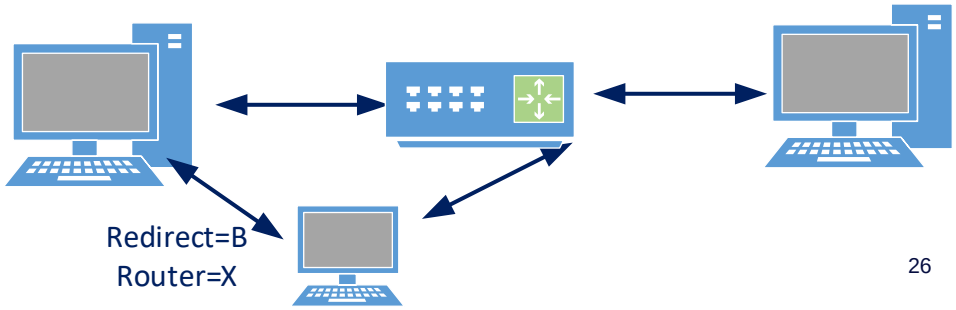
ICMP Source Quench **с**ообщение Type 4 используется для снижения скорости передачи данных и служит для ограничения частоты отправления дейтограммы. Если сообщение инициировано маршрутизатором, то это означает о переполнении буфера очереди, если хостом о переполнении окна получения. В этом случае, отправитель должен уменьшить скорость или приостановить отправку дейтограмм до тех пор, пока не перестанет получать сообщения такого типа. Однако в большинстве узлов сообщения типа Source Quench не используются, так как возможна фальсификация сообщений злоумышленником с целью помешать отправке данных с атакуемого узла.

Возможная атака: Данные сообщения могут использоваться для нарушения связи между отправителем и получателем, путем отправки сообщения о невозможности принять пакеты с данными.

Безопасность ICMP

Redirect. Сообщение Redirect – переадресовать направляется отправителю промежуточным узлом при наличии маршрута лучшего, чем тот, который был выбран ранее. Например:

- Узел А подключенный к маршрутизаторам С1 и С2 отправляет дейтограмму узлу В через маршрутизатор С1.
- Маршрутизатор С1, получив дейтограмму определяет, что рациональнее доставлять дейтограмму через маршрутизатор С2. Поэтому С1 направляет узлу В полученную дейтограмму, а узлу А – сообщение Redirect, содержащее IP-адрес найденного узла.
- Узел А, получив сообщение Redirect воспользуется новой маршрутизацией лишь некоторое время, а затем возвращается к предыдущей.
- ***Router Advertisement/Solicitation*** используются узлом для получения информации об адресах маршрутизаторов к которым он подключен. Для этого узлом формируется широковещательное сообщение ICMP типа 10 (Router Solicitation). Маршрутизатор, получив данное сообщение посылает узлу ответ– сообщение ICMP типа 9 (Router Advertisement), содержащее адрес одного или нескольких маршрутизаторов и значения их приоритетов.
- Сообщение Router Advertisement может использоваться злоумышленником для навязывания атакуемому узлу ложного маршрута или конфигурирования таблиц маршрутизации узла



Безопасность ICMP

Address Mask Request/Reply. Сообщения Address Mask Request Address Mask Reply (17 и 18) используются узлом для получения маски сети, в которой он находится. Для этого узлом генерируется сообщение Address Mask Request, в ответ на которое маршрутизатор отправляет сообщение Address Mask Reply с записанным значением маски той сети откуда пришел запрос.

Сообщения Address Mask Request Address Mask Reply могут использоваться злоумышленником незаконно подключенным к сети для определения маски сети, или для навязывания узлу неверной сетевой маски, лишив его тем самым возможности полноценно работать в сети.

•

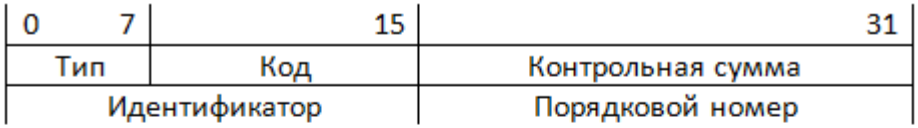


Рис. Запрос адресной маски

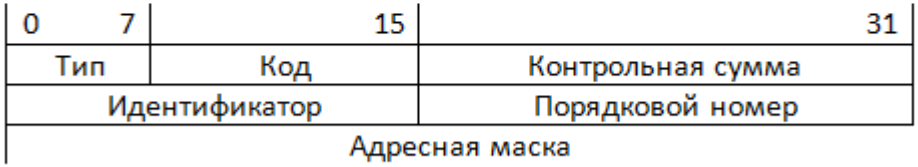


Рис. Отклик на запрос адресной маски