DNS

Domain Name System — система доменных имён

Определения

- Домен
- Поддомен
- Ресурсная запись
- Зона
- Делегирование
- DNS-сервер
- DNS-клиент
- Авторитетность
- DNS-запрос

Интерфейс командной строки для обращения к системе DNS

- ***nslookup*** *[-параметры] [узел] [сервер]*

Неавторитетный ответ	Авторитетный ответ
nslookup tsu.ru Server: google-public-dns-a.google.com Address: 8.8.8.8 Non-authoritative answer: Name: tsu.ru Address: 92.63.64.84	*nslookup tsu.ru mx.tsu.ru* Server: mx.tsu.ru Address: 82.200.70.8 Name: tsu.ru Address: 92.63.64.84

Ошибки nslookup

Сообщение об ошибке	Причина
Connection refused (В соединении отказано)	Невозможно установить соединение с сервером DNS. Эта ошибка обычно возникает в случае подключения к серверу, разрешающему передачу зоны только определенным серверам
Format error (Ошибка формата)	Сервер DNS обнаружил ошибку в пакете запроса команды nslookup
Network is unreachable (Сеть недоступна)	Невозможно установить соединение с сервером DNS. Постарайтесь выяснить существование маршрутизации для сети сервера DNS, отправив тестовый эхо-пакет узлу в подсети сервера DNS
No response from server (Нет ответа сервера)	На указанном (в параметрах команды или в свойствах протокола TCP/IP) узле не запущена служба DNS

Ошибки nslookup

Сообщение об ошибке	Причина
Nonexistent domain (Несуществующий домен)	Невозможно найти записи о запрошенном доменном имени
Refused (Отказано)	Сервер преобразования имен ответил отказом на запрос утилиты nslookup. Причина аналогична ошибке Connection refused
Server failure (Отказ сервера)	Ошибка или нарушение целостности файла с данными зоны на сервере DNS.
Timed out (Превышение таймаута)	Сервер DNS не ответил в течение указанного промежутка времени и интервала повторного запроса (Retry Interval). По умолчанию таймаут равен 5 секундам. Интервал повтора равен 4. Это означает, что утилита будет ожидать ответа в течение 20 секунд перед тем, как выдать это сообщение об ошибке

Статическая маршрутизация

Вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

Сетевой шлюз

- **Сетевой шлюз** (англ. gateway) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

При задании статического маршрута указывается

- Адрес сети (на которую маршрутизируется трафик), маска сети
- Адрес шлюза, который отвечает за дальнейшую маршрутизацию (или подключен к маршрутизируемой сети напрямую)
- (опционально) метрика (иногда именуется также "ценой") маршрута. При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой

Достоинства статической маршрутизации

- Лёгкость отладки и конфигурирования в малых сетях.
- Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации).
- Мгновенная готовность (не требуется интервал для конфигурирования/подстройки).
- Низкая нагрузка на процессор маршрутизатора.
- Предсказуемость в каждый момент времени.

Недостатки статической маршрутизации

- Очень плохое масштабирование.
- Низкая устойчивость к повреждениям линий связи.
- Отсутствие динамического балансирования нагрузки

Windows

route *[**-f**] [**-p**] [Command [Destination] [**mask** Netmask] [Gateway] [**metric** Metric]] [**if** Interface]]*

Параметры утилиты route

- -f : Очищает таблицу маршрутизации
- -p : В сочетании с командой add добавляет постоянный маршрут в таблицу, без этого параметра маршрут будет удален после перезапуска драйвера TCP/IP. В сочетании с командой print распечатывает все постоянные маршруты. Для остальных команд игнорируется.
- Command : Одна из возможных команд. Список ниже.
  - add добавляет маршрут
  - change модифицирует существующий маршрут
  - delete удаляет маршрут(ы)
  - print распечатывает маршруты

Параметры утилиты route

- Destination : Определяет назначение для маршрута. Назначение может иметь форму IP адреса хоста, IP адреса сети, где адрес хоста установлен в 0, или 0.0.0.0 для маршрута по умолчанию.
- mask Netmask задает маску подсети. Может быть любой корректной сетевой маской, 255.255.255.255 для единичного хоста, или 0.0.0.0 для маршрута по умолчанию. Если параметр отсутствует, используется маска 255.255.255.255. На комбинацию маски и назначения накладывается ограничение. Если в маске некоторый бит установлен в 0, соответствующий бит в назначении не может быть установлен в 1.
- Gateway : адрес шлюза
- metric Metric : Целое число (от 1 до 9999) метрика маршрута, используемая когда имеется выбор между несколькими маршрутами в таблице маршрутов, ведущими к искомому назначению. Выбирается маршрут с наименьшей метрикой.
- if Interface : индекс (десятичное или шестнадцатеричное число) сетевого интерфейса используемого для прокладки данного маршрута. Список имеющихся в системе интерфейсов можно увидев выполнив команду route print. Если параметр опущен, интерфейс выбирается на основании адреса шлюза.

Linux

route del *[**-net**|**-host**] цель [**gw** шлюз] [**netmask** маска_сети] [**metric** N] [[**dev**] интерфейс]*

Параметры утилиты route

- del Удалить маршрут.
- add Добавить новый маршрут.
- цель Целевая сеть или узел. Вы можете указать IP-адрес в десятично-точечной нотации или имя узла/сети.
- -net цель является сетью.
- -host цель является узлом.

Параметры утилиты route

- netmask маска_сети При добавлении маршрутов к сетям указывается сетевая маска.
- gw шлюз
- metric M - Задаёт в поле метрики таблицы маршрутизации значение M (используется демонами маршрутизации).
- dev интерфейс - Принудительно связать маршрут с указанным интерфейсом, поскольку ядро ОС в ином случае определит его самостоятельно (проверкой уже существующих маршрутов и устройств, после чего маршрут будет добавлен).

Диагностика проблем маршрутизации

- **ICMP** (англ. Internet Control Message Protocol — протокол межсетевых управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи диагностических сообщений и сообщений об ошибках, возникших при передаче данных.

Ping

- **Ping** — утилита для проверки соединений в сетях на основе TCP/IP.

Windows

ping <имя_назначения или адрес_IP> *[-a] [-i <TTL>] [-j <список_узлов>] [-n <счетчик>] [-t]*

```
C:\Users\predictor>ping tsu.ru

Pinging tsu.ru [92.63.64.84] with 32 bytes of data:
Reply from 92.63.64.84: bytes=32 time=1ms TTL=61
Reply from 92.63.64.84: bytes=32 time<1ms TTL=61
Reply from 92.63.64.84: bytes=32 time<1ms TTL=61
Reply from 92.63.64.84: bytes=32 time<1ms TTL=61

Ping statistics for 92.63.64.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Параметры команды ping

Параметр	Использование
<имя_назначения или адрес_IP>	Обязательный параметр. Указывает имя назначения и адрес IP
-a	Определение адресов по именам узлов
-i <TTL>	Указывает время жизни (TTL) тестового запроса; по умолчанию используется значение 128; этот параметр позволяет установить значение до 255, что позволяет тестовому пакету пройти 255 маршрутизаторов и быть удаленным 256 маршрутизатором.
-j <список_узлов>	Позволяет указать промежуточные узлы в виде адресов IP, разделенных пробелами (список_узлов). не более девяти узлов.
-n <счетчик>	Используется для указания количества тестовых запросов, которые отправляются командой ping.
-t	Заставляет команду ping непрерывно отправлять тестовые запросы, пока выполнение команды не будет прервано комбинацией клавиш <Ctrl+C>.

Linux

ping *[-**bv**] [-**c** количество] [-**i** интервал] [-**t** ttl] [-**w** ограничение-на-время-работы] назначение*

```
predictor@prog:~$ ping -c 5 tsu.ru
PING tsu.ru (92.63.64.84) 56(84) bytes of data.
64 bytes from 92.63.64.84: icmp_req=1 ttl=62 time=0.368 ms
64 bytes from 92.63.64.84: icmp_req=2 ttl=62 time=0.422 ms
64 bytes from 92.63.64.84: icmp_req=3 ttl=62 time=0.502 ms
64 bytes from 92.63.64.84: icmp_req=4 ttl=62 time=0.466 ms
64 bytes from 92.63.64.84: icmp_req=5 ttl=62 time=0.461 ms

--- tsu.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.368/0.443/0.502/0.052 ms
```

ОПЦИИ

- -**b** - Разрешить использование широковещательного адреса в качестве целевого.
- -**c** *количество* - Остановить работу после передачи заданного количества пакетов ECHO_REQUEST. Если задано *ограничение-на-время-работы,* программа будет ждать указанное количество ответных пакетов ECHO_REPLY в указанный период.
- -**i** *интервал* - Интервал в секундах между отправкой пакетов. По умолчанию 1 секунда.
- -**t** *ttl* - Время актуальности пакета IP (ttl - Time to Live).
- -**w** *ограничение-на-время-работы* - Время, по истечении которого ping завершит свою работу независимо от количества посланных и принятых пакетов.

Traceroute

Утилита, предназначенная для определения маршрутов следования данных в сетях *TCP/IP*. **Traceroute** может использовать разные протоколы передачи данных в зависимости от операционной системы. Компьютеры с ОС Windows используют *ICMP*, с ОС Linux по умолчанию *UDP*.

Windows

tracert <*имя_назначения или адрес_IP*>

[-***d***]

[-***h*** <*максимальное_количество_переходов*>]

[-***j*** <*список_узлов*>]

[-***w*** <*таймаут*>]

Windows

```
C:\Users\predictor>tracert tsu.ru

Tracing route to tsu.ru [92.63.64.84]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  firewall.uvaresearch.com [192.168.0.1]
  2    <1 ms     1 ms     1 ms  gate.net.tomline.ru [83.172.0.129]
  3     4 ms     1 ms     1 ms  tsu.tomline.ru [213.183.97.38]
  4     3 ms     2 ms     2 ms  92.63.64.84

Trace complete.
```

Параметры команды **tracert**

Параметр	Использование
<имя_назначения или адрес_IP>	Обязательный параметр. Доменное имя точки назначения или адрес IP
-**d**	Ускоряет выполнение команды tracert за счет отказа от преобразования адресов IP маршрутизаторов в доменные имена
-**h** *<максимальное_количество_переходов>*	Используется для указания максимального количества переходов по пути к точке назначения. По умолчанию используется значение 30.
-**j** *<список_узлов>*	Позволяет указать промежуточные точки назначения в виде списка адресов IP, разделенных пробелами (список_узлов). до девяти промежуточных узлов.
-**w** *<таймаут>*	Используется для указания времени (в миллисекундах) ожидания ответа. Если ответ не был получен за указанное время, отображается символ (*). По умолчанию используется значение 4000 (4 секунды).

Linux

traceroute [-**el**] [-**m** *max_ttl*] [-**P** *proto*] [-**p** *port*] [-**q** *nqueries*] [-**w** *waittime*] [-**z** *pausemsecs*] **host**

```
predictor@prog:~$ traceroute tsu.ru
traceroute to tsu.ru (92.63.64.84), 30 hops max, 60 byte packets
 1  mail.fpmk.tsu.ru (92.63.67.200)  0.153 ms  0.153 ms  0.150 ms
 2  92.63.65.21 (92.63.65.21)  0.747 ms  0.750 ms  0.832 ms
 3  * * *
 4  * * *
 5  * * *
…
```

Опции **traceroute**

-e режим обхода файерволов: используются фиксированные номера портов, не выполняется инкремент для каждого пакета

-I используется пакет ICMP ECHO вместо UDP, используемого по умолчанию

-m *max_ttl* максимальное число переходов на пути к назначению, по умолчанию 30

-P *proto* использовать пакеты указанного протокола (UDP, TCP, GRE and ICMP)

-p *port* номер порта в для заданного протокола, используется с предыдущим параметром

Опции **traceroute**

-q *nqueries* число попыток запросов для одного перехода, по умолчанию 3

-w *waittime* время ожидания ответа (в секундах) на запрос, по умолчанию 5 секунд

-z *pausemsecs* пауза (в миллисекундах) между запросами, по умолчанию 0, рекомендуется использовать значение 500 (1/2 секунды), если какой-либо маршрутизатор на пути пакета ограничивает частоту запросов

host IP адрес или доменное имя назначения

Linux

```
predictor@prog:~$ sudo traceroute -I tsu.ru

traceroute to tsu.ru (92.63.64.84), 30 hops max, 60 byte packets

 1  mail.fpmk.tsu.ru (92.63.67.200)  0.121 ms  0.129 ms  0.138 ms

 2  92.63.65.21 (92.63.65.21)  0.676 ms  0.844 ms  0.857 ms

 3  92.63.64.84 (92.63.64.84)  0.478 ms  0.492 ms  0.503 ms
```

Whois

- **WHOIS** (от англ. who is) — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.

Whois

- Протокол подразумевает архитектуру «клиент-сервер» и используется для доступа к публичным серверам баз данных (БД) регистраторов IP-адресов и регистраторов доменных имён.

http://whois.net/ip-address-lookup/92.63.65.21

```
[Querying whois.arin.net]
[Redirected to whois.ripe.net:43]
[Querying whois.ripe.net]
[whois.ripe.net]

% Information related to '92.63.64.0 - 92.63.68.255'

inetnum:        92.63.64.0 - 92.63.68.255
netname:        TSUNET
descr:          Tomsk State University
country:        RU
admin-c:        AY254-RIPE
tech-c:         AY254-RIPE
status:         SUB-ALLOCATED PA
mnt-by:         tsunet-mnt
source:         RIPE # Filtered

person:         Anatoly Yuzefovich
address:        Tomsk State University
address:        Lenin avenue, 36
address:        Tomsk
address:        Russia
phone:          +73822529696
nic-hdl:        AY254-RIPE
mnt-by:         ZSTTK-MNT
source:         RIPE # Filtered

% Information related to '92.63.64.0/20AS8510'

route:          92.63.64.0/20
descr:          Tomsk State University
origin:         AS8510
```