КПИ им. Игоря Сикорского, каф. микроэлектроники.
М. Р. Домбругов. Информатика-1.
Персональные компьютеры и основы сетевых технологий

Лекция 7.
DNS. Диагностика сети.
5-й (сеансовый) уровень модели OSI

9 ноября 2020

DNS – Domain Name System

Система доменных имен (Domain Name System, DNS) служит для преобразования доменного имени в IP-адрес и наоборот.

Напр.:

me.kpi.ua → 77.47.133.104
mido.kiev.ua → 212.111.212.227

Имя и IP-адрес не тождественны: одному IP-адресу может соответствовать несколько доменов (**«виртуальный хостинг»**):

uran.ua → 212.111.212.227
peano.uran.ua → 212.111.212.227

И наоборот, одному имени может быть сопоставлено множество IP-адресов (для балансировки нагрузки)

IP-адрес устройства можно сравнить с номером телефона, доменное имя – с именем абонента, а систему DNS – с телефонной книгой.

DNS: доменные имена

Доменное имя

– обозначение для адресации узлов интернета и расположенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты…) в удобной для человека форме.

Доменное имя имеет иерархическая структуру,
напр. **mido.kiev.ua** или **me.kpi.ua**.

Вверху иерархии находится **корневой домен,**
имеющий идентификатор «.» (точка),
ниже идут домены первого уровня (**top-level domain, TLD**),
затем – домены второго уровня, третьего и т. д.

Точку корневого домена обычно можно не указывать.

Субдомен – подчинённый домен,напр.,
kpi.ua – субдомен домена **ua**, а **me.kpi.ua** – домена **kpi.ua**.

Макс. длина доменного имени (вместе с точками) = 254 символа.

DNS: доменные имена

Для обеспечения уникальности доменные имена можно использовать только после их регистрации.

Регистратор доменных имен первого уровня (TLD) – международная некоммерческая организация **ICANN (Internet Corporation for Assigned Names and Numbers),** действующая по контракту с IANA.

На сегодня зарегистрировано более 1500 TDL

Исторически первые 6 TLD:

.com	веб-сайты коммерческих организаций
.net	административные веб-сайты Интернета
.org	некоммерческие организации
.gov	правительственные организации США
.mil	военные организации США
.edu	образовательные учреждения

DNS: доменные имена

Некоторые национальные TLD:

.br	Бразилия
.cn	Китай
.de	Германия
.fr	Франция
.jp	Япония
.ru	Россия
.tw	Тайвань
.ua	**Украина**
.zw	Зимбабве

Некоторые корпоративные TLD:

.aaa	American Automobile Association
.basketball	FIBA
.bmw	BMW
.cern	CERN
.delta	Delta Air Lines
.ford	Ford Motor Company
.ibm	IBM
.microsoft	Microsoft
.mit	Massachusetts Institute of Technology
.mormon	The Church of Jesus Christ of Latter-day Saints (LDS Church)
.nike	Nike
.saxo	Saxo Bank
.windows	Microsoft

DNS: доменные имена

Домены бывают **публичные**, в которых регистрация субдоменов производится без ограничений,
и **приватные**, принадлежащие предприятию или частному лицу, где только владелец вправе регистрировать субдомены.

Регистратор доменных имен в зоне **.ua** – ТОВ «Хостмастер».

В зоне **.ua** приватные субдомены второго уровня регистрируются только для владельцев зарегистрированных торговых марок (напр. **kpi.ua, uran.ua**).

В зоне **.ua** имеются ок. 50 публичных доменов второго уровня, регистрация в которых производится без ограничений:
тематические: **com.ua, net.ua, org.ua** …
географические: **kiev.ua, poltava.ua, lv.ua** …

Напр.: **mido.kiev.ua** – приватный домен в зоне **kiev.ua**, зарегистрированный без торговой марки.

DNS: регистрация домена

Регистрация домена – это внесение **ресурсных записей (resource records, RR)** о нем на один из DNS-серверов.

Каждая RR содержит поля:

- **NAME** – доменное имя, к которому относится данная RR,
- **TYPE** – определяет формат и назначение RR,
- CLASS – устарело и не используется,
- **TTL** (Time To Live) – срок жизни, время хранения этой RR в кэше неответственного DNS-сервера,
- RDLEN – длина поля данных,
- RDATA – поле данных, Его формат и содержание зависит от типа записи.

Типы DNS-записей

Наиболее важные типы DNS-записей:

- **Запись A** (**a**ddress record) связывает имя хоста с IPv4-адресом. Если на этом домене развернут веб-сервер, то он доступен по этому адресу с использованием протокола HTTP (HyperText Transfer Protocol) по порту 80.
- **Запись MX** (**m**ail e**x**changer) содержит имя почтового сервера, обслуживающего домен. По данному имени с помощью A-записи будет определяться IP-адрес для маршрутизации электронной почты с использованием протокола SMTP (Simple Mail Transfer Protocol) по порту 25.
- **Запись NS** (**n**ame **s**erver) указывает на DNS-сервер данного домена в случае, если он содержит поддомены.

Распределённая база данных DNS поддерживается с помощью иерархии взаимодействующих между собой DNS-серверов.

Корневые DNS-серверы

Корневой DNS-сервер ответственный за корневую зону.
Их в мире 13, а вместе с репликами – 1329 (в Киеве 7).

Имя хоста	IP-адреса		Управляющая организация
a.root-servers.net	198.41.0.4,	2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201,	2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12,	2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13,	2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10,	2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241,	2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4,	2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53,	2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17,	2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30,	2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129,	2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42,	2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33,	2001:dc3::35	WIDE Project

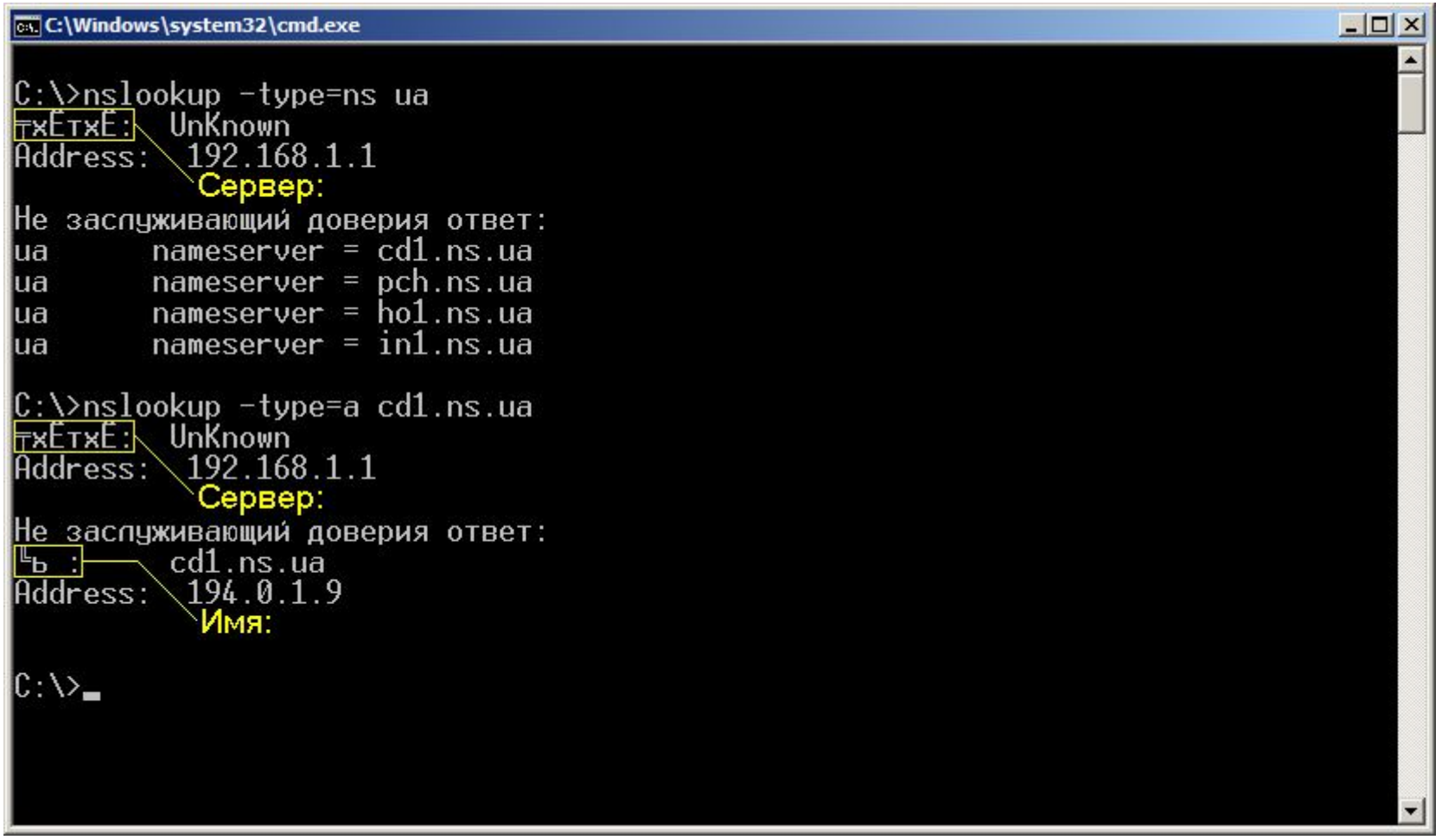
Иерархия DNS-серверов

Каждый DNS-сервер может делегировать ответственность за поддомен другому серверу (с административной точки зрения – другой организации или человеку), который будет ответственным за актуальность информации «своей» части доменного имени.

Посмотреть записи из этой распределенной базы можно при помощи команды

nslookup –type=<TYPE> <NAME>

Записи о зоне ua на корневых NS



Записи о зоне ua на корневых NS

Пример: NS-записи о домене **.ua** на корневых DNS-серверах

https://www.iana.org/domains/root/db/ua.html

Name Servers

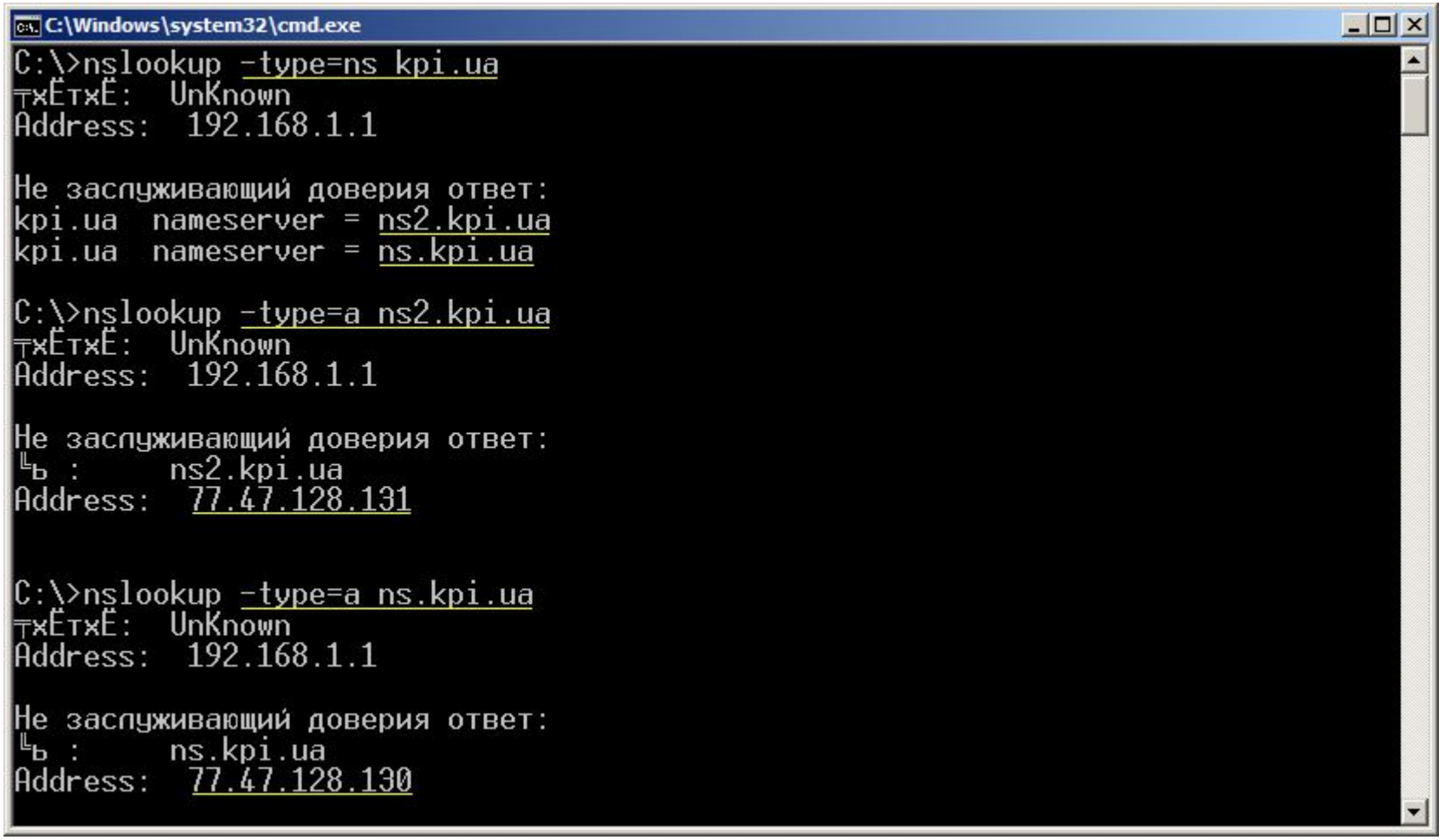
HOST NAME	IP ADDRESS(ES)
ho1.ns.ua	195.47.253.1 2001:67c:258:0:0:0:0:1
pch.ns.ua	204.61.216.12 2001:500:14:6012:ad:0:0:1
cd1.ns.ua	194.0.1.9 2001:678:4:0:0:0:0:9
in1.ns.ua	74.123.224.40 2604:ee00:0:101:0:0:0:40

Registry Information

URL for registration services: http://hostmaster.ua/

На DNS-серверах домена **.ua** хрянятся записи о доменах **kpi.ua, uran.ua, kiev.ua** и других субдоменах этой зоны.

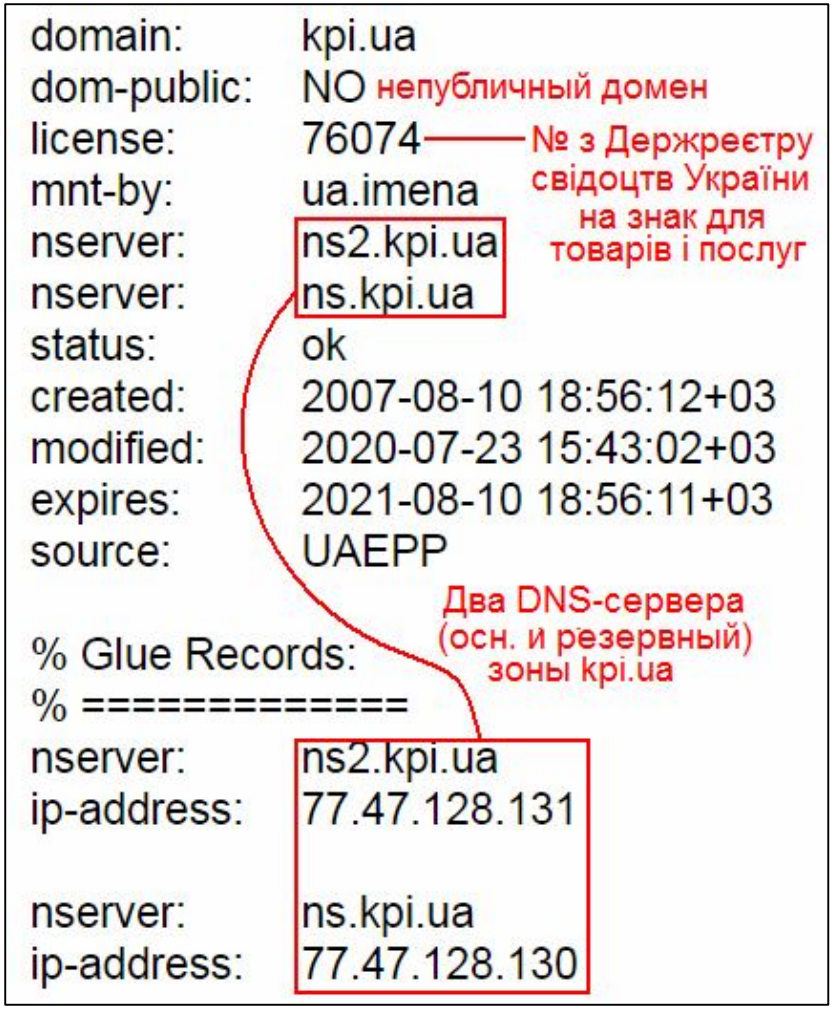
Записи о зоне kpi.ua на NS зоны ua



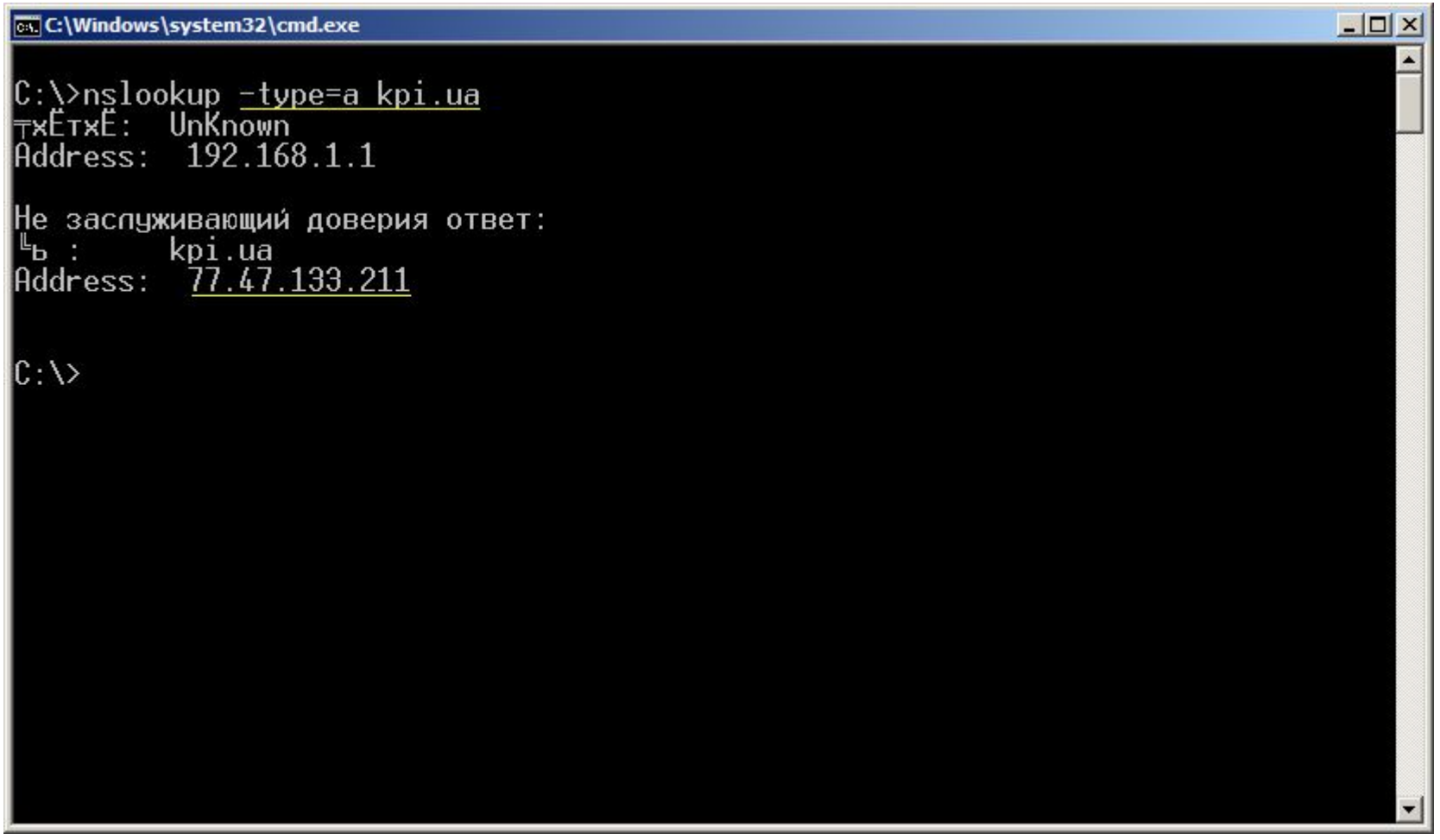
Записи о зоне kpi.ua на NS зоны ua

Пример: NS-записи о домене **kpi.ua** на DNS-серверах регистратора зоны **.ua**

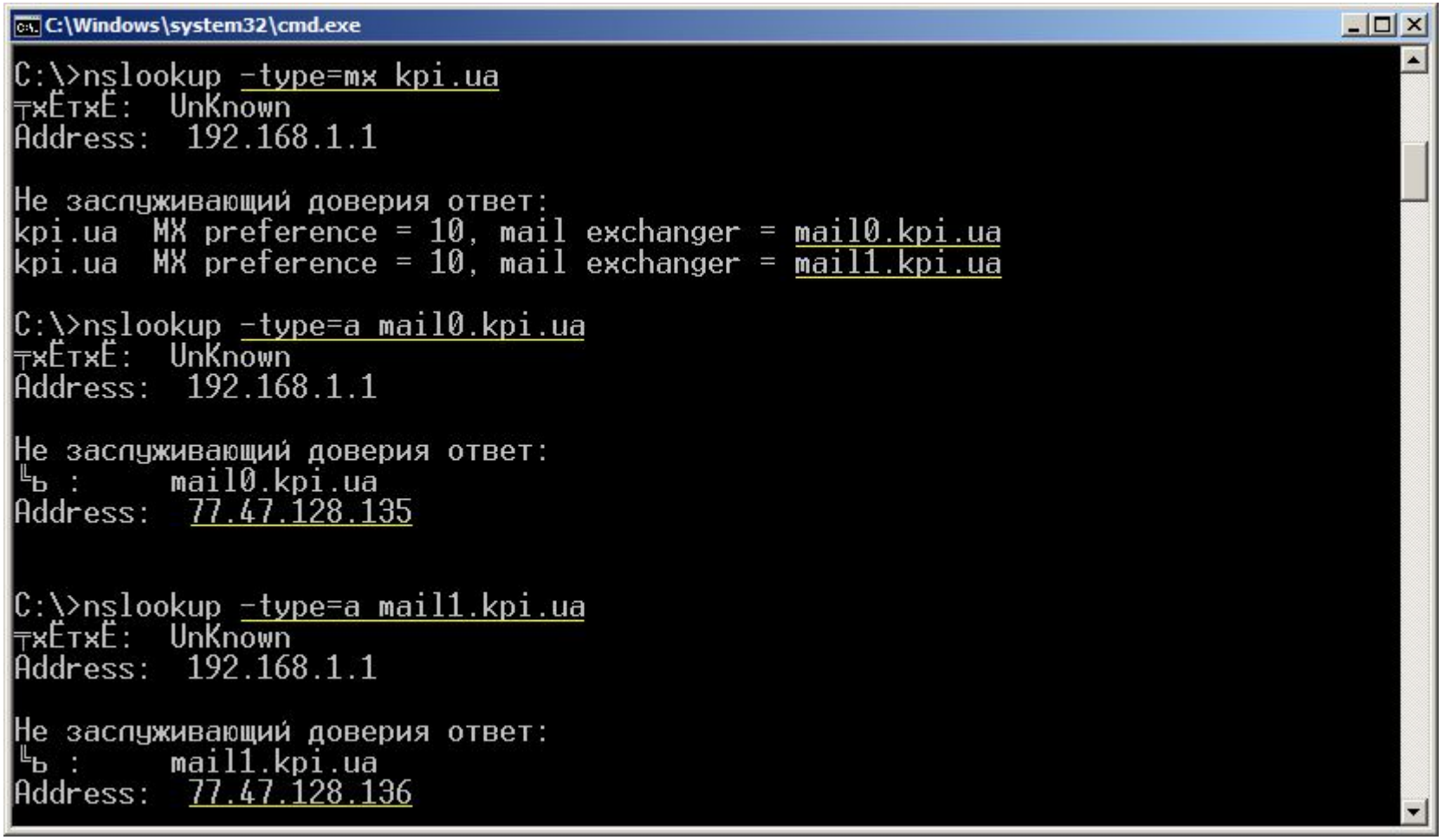
https://hostmaster.ua/?domadv



Записи о зоне kpi.ua на NS зоны ua



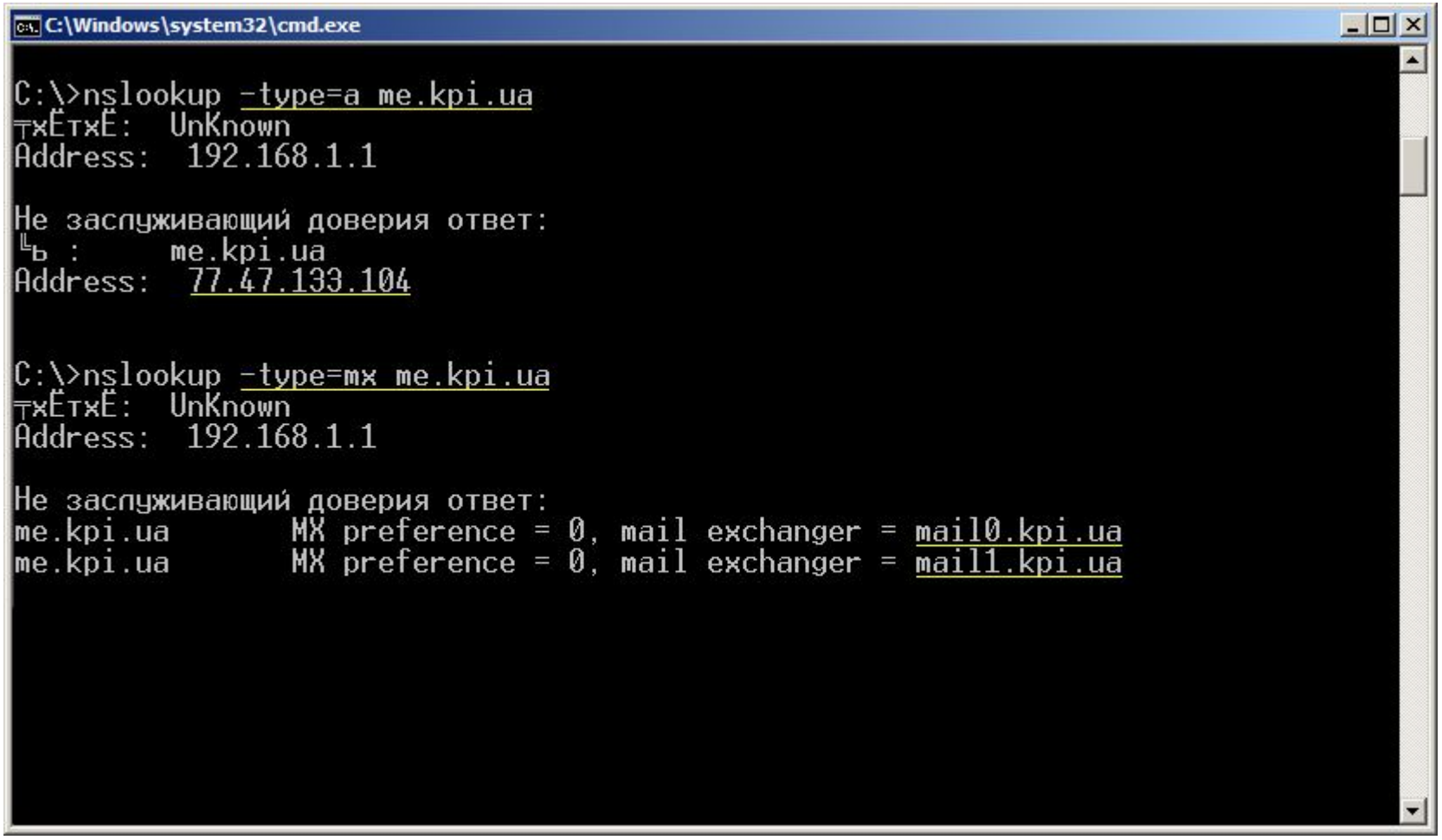
Записи о зоне kpi.ua на NS зоны ua



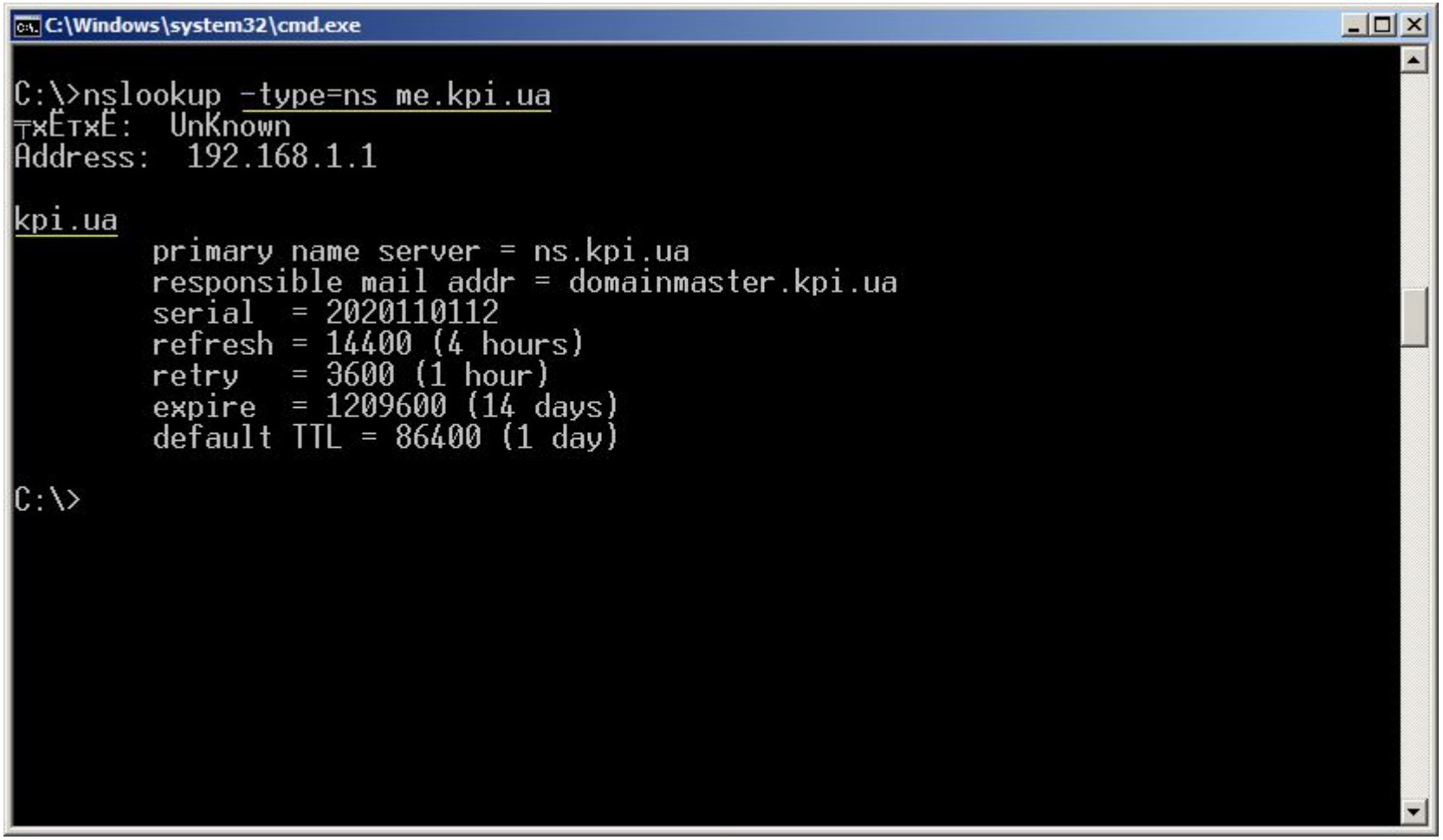
Субдомены зоны kpi.ua

На DNS-серверах домена **kpi.ua** хрянятся записи о доменах **me.kpi.ua, fel.kpi.ua** и других субдоменах этой зоны.

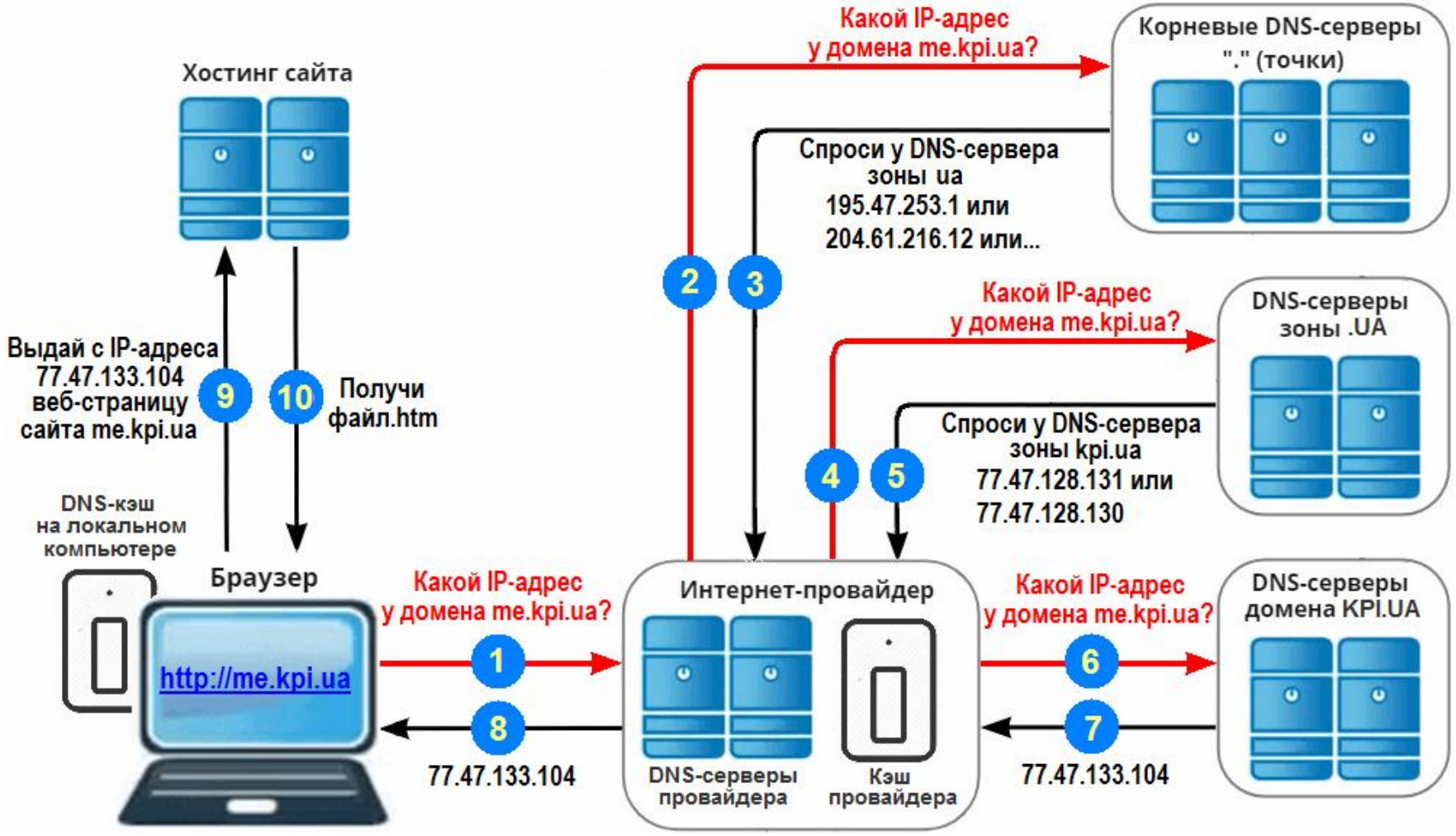
Субдомены зоны kpi.ua



Субдомены зоны kpi.ua



Запрос о DNS-записи типа «A» (обмен UDP-датаграммами на порт 53)



Ключевые характеристики DNS

- **Иерархическая структура:** все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать это другим узлам.
- **Распределённость администрирования:** ответственность за разные части структуры несут разные люди или организации.
- **Распределённость хранения информации:** каждый узел сети *обязательно* хранит данные, относящиеся к его зоне ответственности, и (возможно) адреса корневых DNS-серверов.
- **Кэширование информации:** узел *может* хранить некоторые данные не из своей зоны ответственности для уменьшения нагрузки на сеть.
- **Резервирование:** за обслуживание своих узлов (зон) обычно отвечают несколько серверов. Поэтому работоспособность системы сохраняется даже в случае сбоя одного из узлов.

Кэширование записей DNS

При обработке запросов все ответы проходят через DNS-сервер, и он получает возможность помещать их в **кэш** – промежуточную область памяти (буфер) для временного хранения данных.

Доступ к данным в кэше осуществляется быстрее, чем их выборка из удалённого источника, однако объём кэша невелик по сравнению с хранилищем исходных данных.

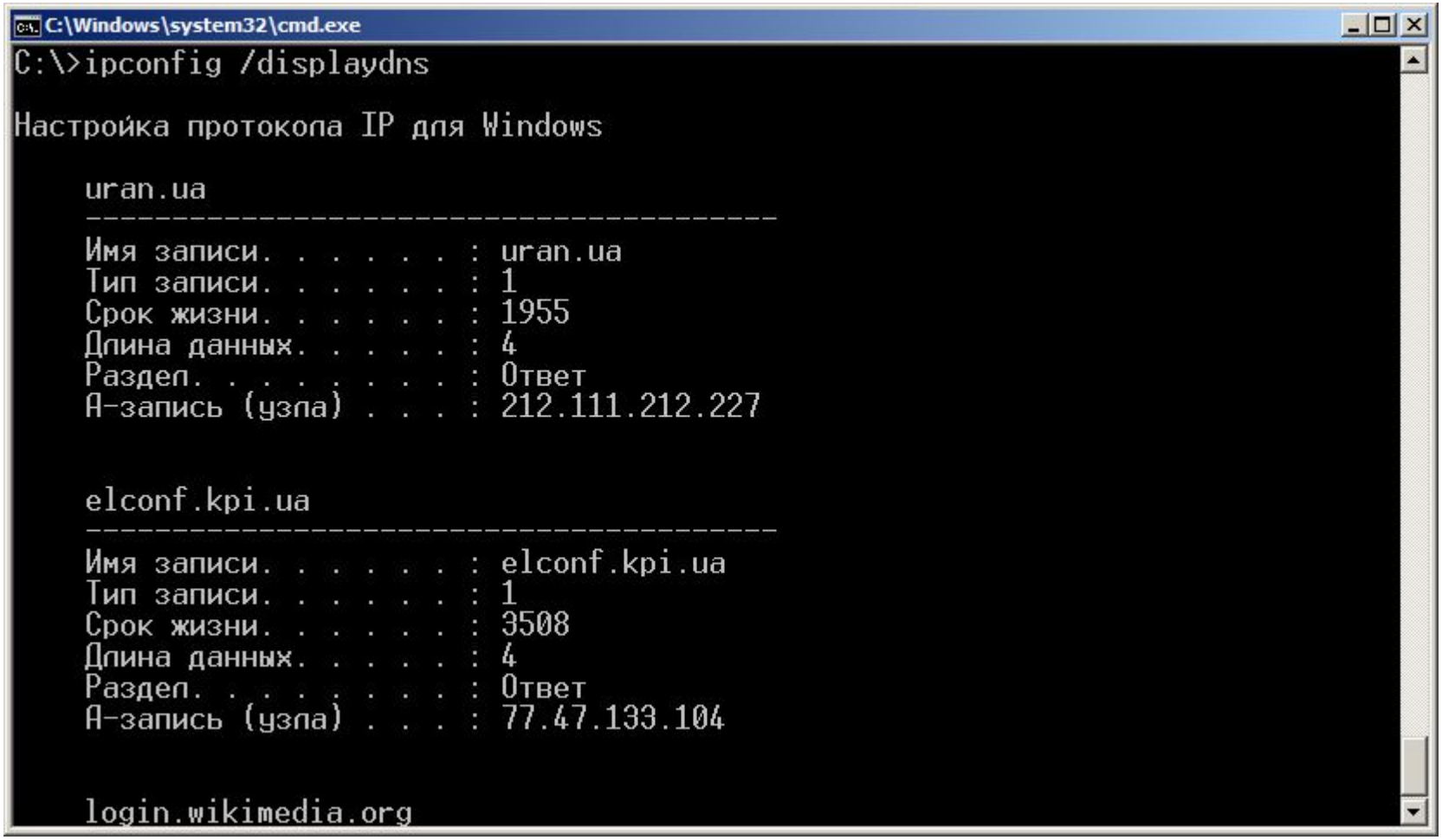
Повторный запрос на те же имена не идёт дальше кэша сервера; обращений к другим серверам не происходит вообще.

Допустимое время хранения ответов в кэше приходит вместе с ответами (поле **TTL** ресурсной записи).

На локальном компьютере также хранится **локальный кэш DNS**.

~70% запросов не доходят до корневых серверов, а получают ответы из промежуточных DNS- кэшей.

Локальный кэш DNS

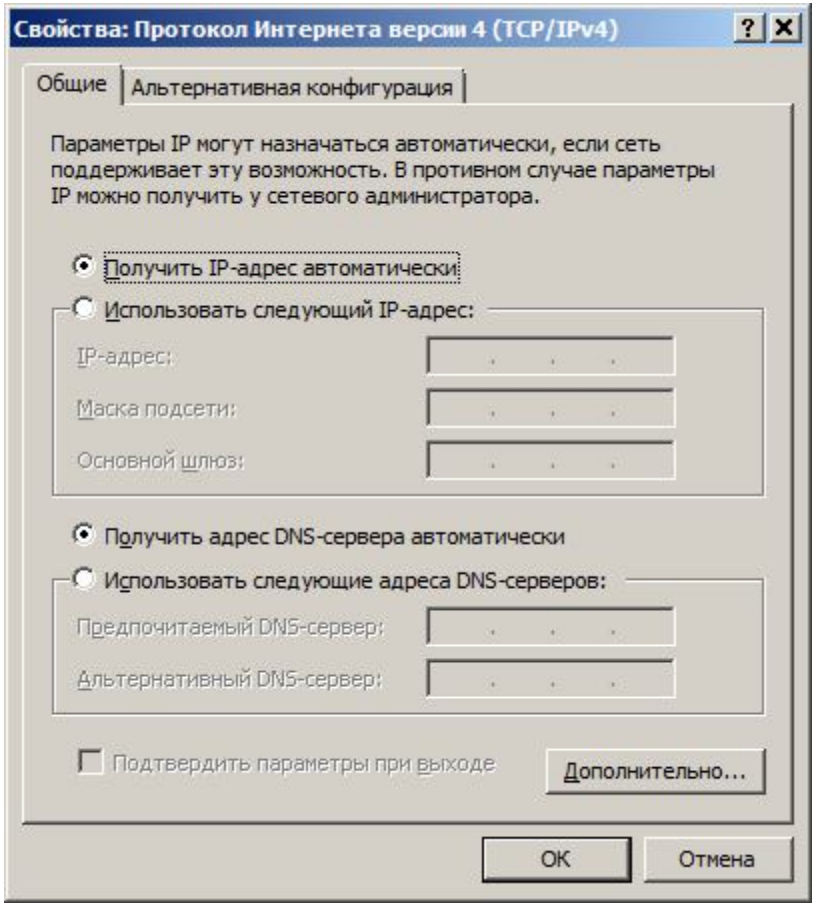


Назначение DNS-сервера узлу

Два способа:

- Вручную на каждом хосте;
- Разместить в сети **DHCP-сервер** и запрашивать параметры при включении хоста у него.

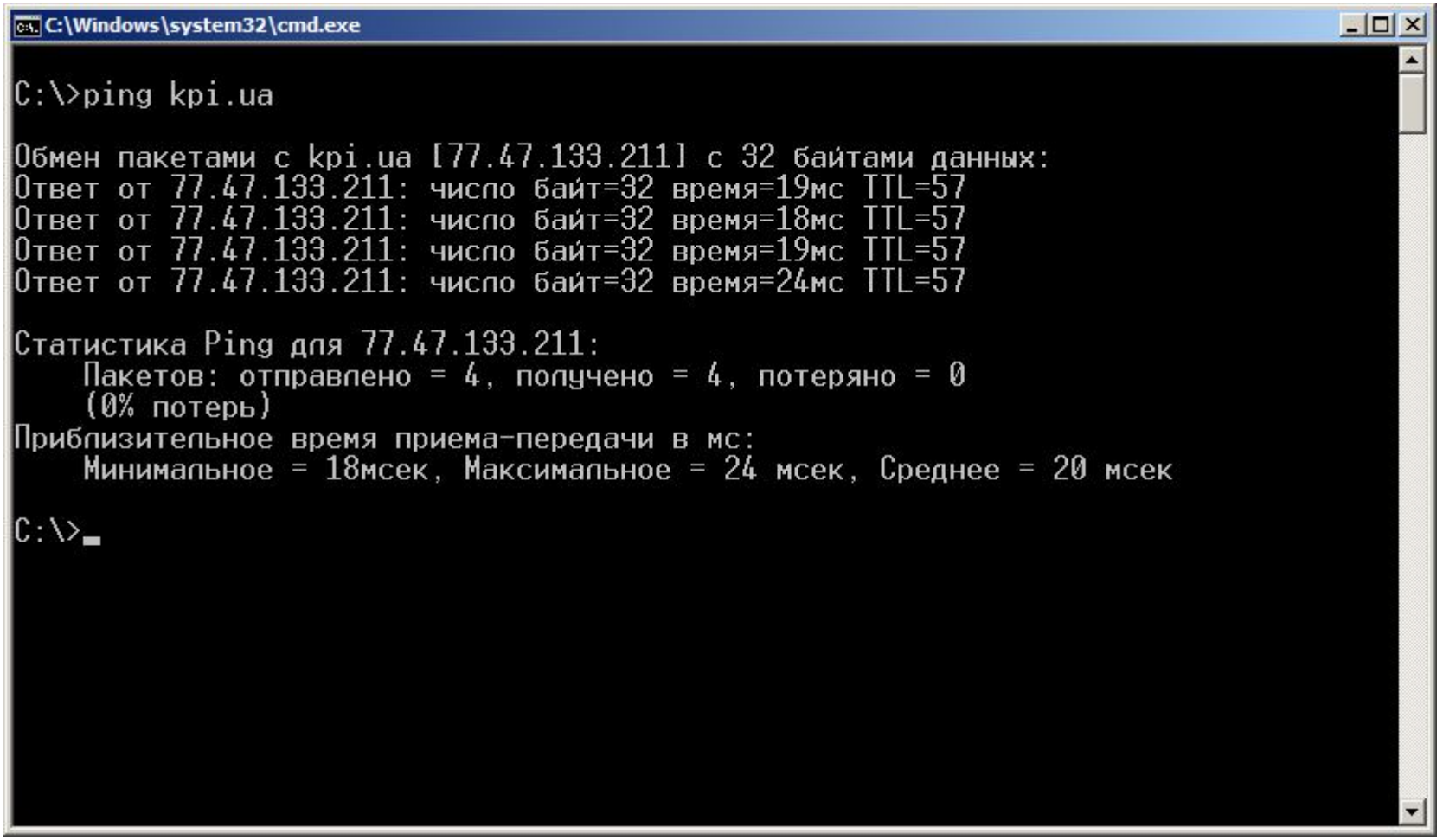
При назначении вручную адрес DNS-сервера должен сообщить администратор сети,
либо можно использовать **публичные DNS-сервера** (напр. от Google **8.8.8.8** и **8.8.4.4**)



DNS

- https://ru.wikipedia.org/wiki/DNS
- https://ru.wikipedia.org/wiki/Доменное_имя
- https://ru.wikipedia.org/wiki/Корневые_серверы_DNS
- https://1cloud.ru/help/dns/dns_basics
- https://habr.com/ru/company/1cloud/blog/309018/
- https://neoserver.ru/kak-rabotaet-dns
- https://hostiq.ua/blog/how-does-dns-work/
- https://jino.ru/help/articles/dns/
- https://timeweb.com/ru/community/articles/chto-takoe-dns-prostymi-slovami
- https://tproger.ru/explain/domain-name-system/

Диагностика сети: доступность узла



Диагностика сети: доступность узла

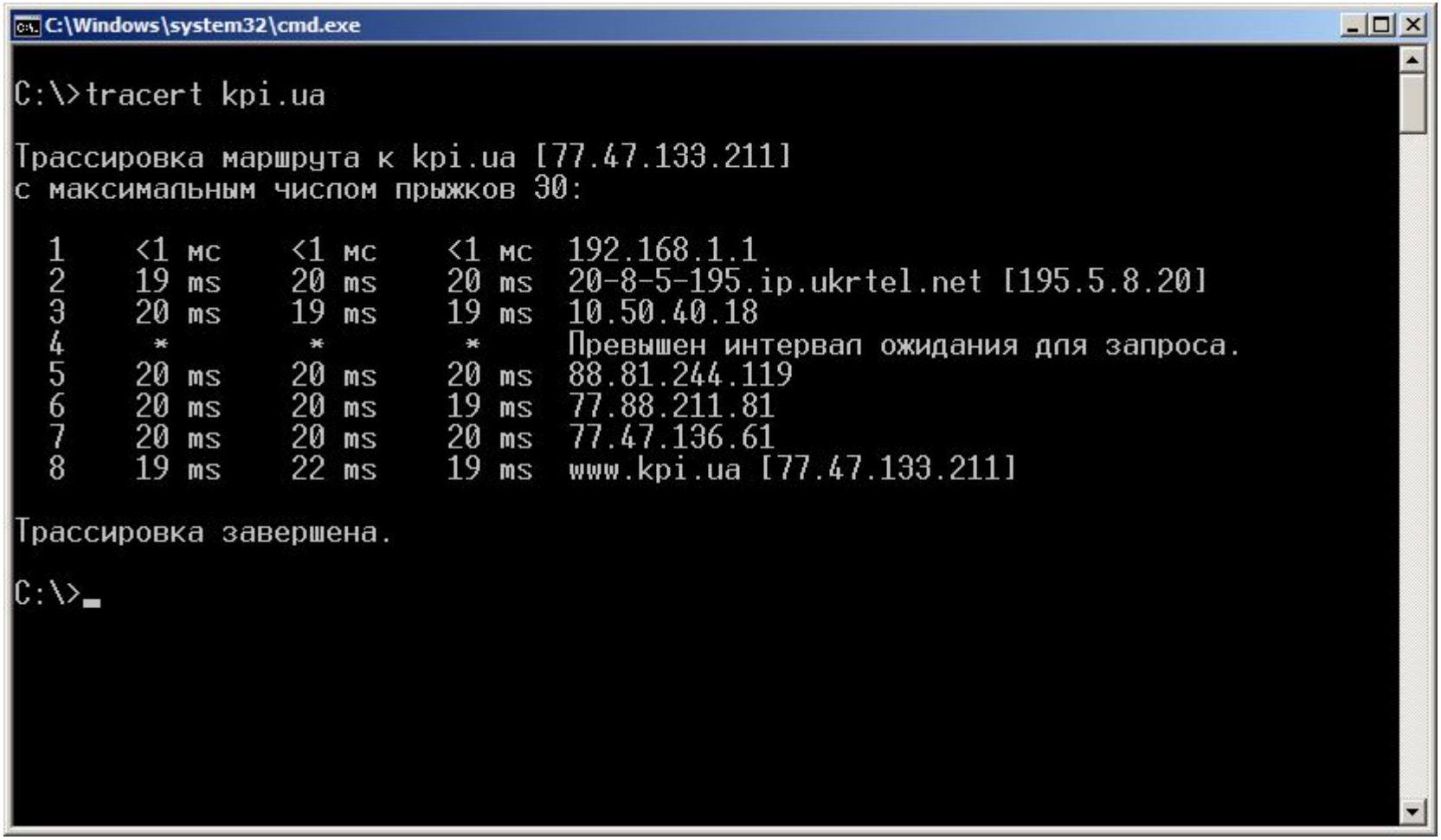
ping 127.0.0.1 – диагностика локального сетевого интерфейса. Если нет ответа, значит, не работает сетевая карта или на компьютере не настроен IP-протокол.

ping <IP-адрес шлюза> – проверка соединения с локальной сетью. Еесли нет ответа, значит, поврежден кабель.

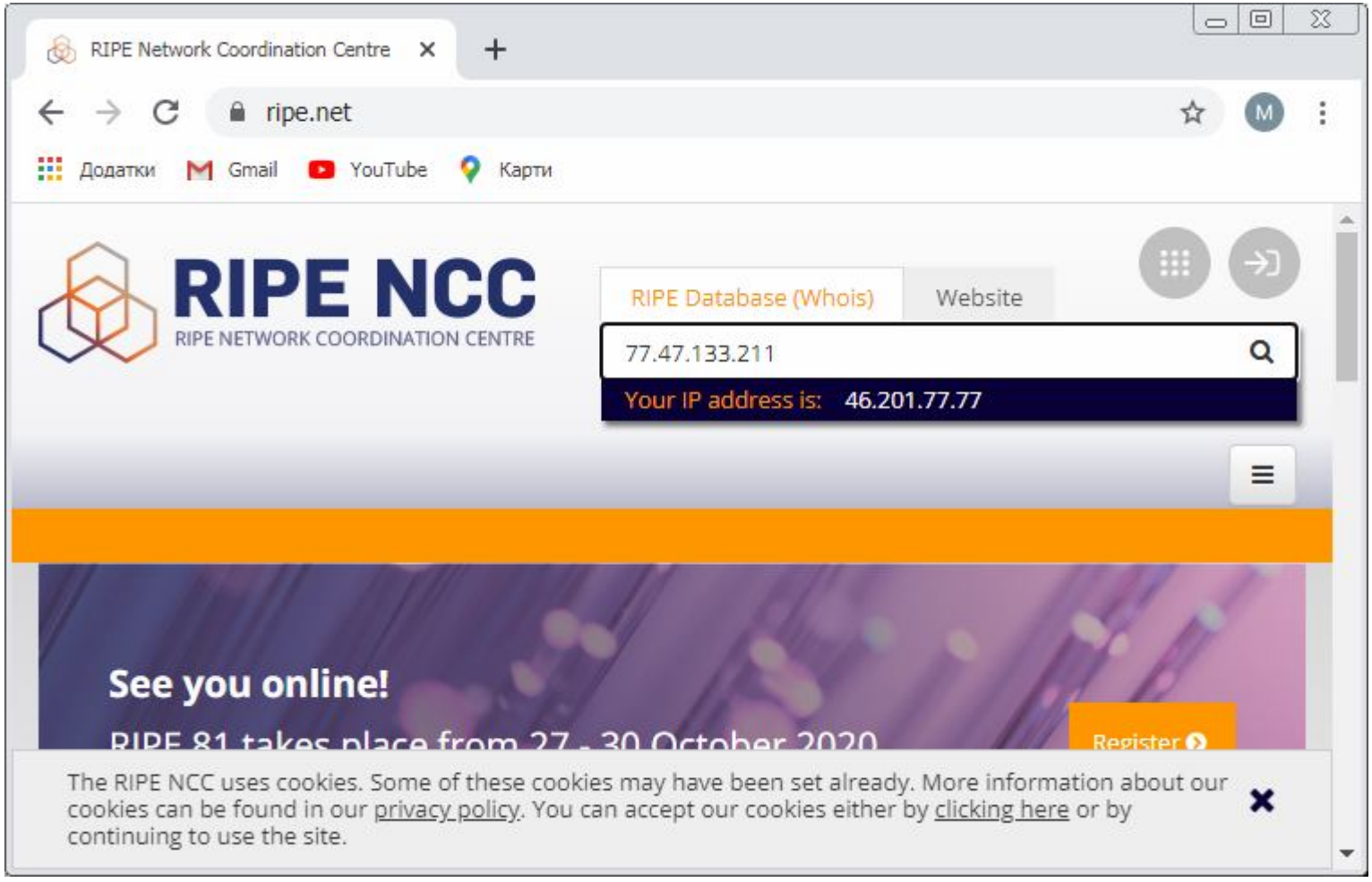
ping <доменное имя> – проверка DNS-сервера. Если нет ответа, а ответ **ping <IP-адрес>** с того же узла поступает, значит, не работает DNS.

Дополнительные возможности: **ping /?**

Диагностика сети: трассировка



Принадлежность IP-адресов



Принадлежность IP-адресов

Ответ от RIPE Database (Whois) https://www.ripe.net/

Responsible organisation: Association of users of Ukrainian Research & Academic Network "URAN"
Abuse contact info: abuse@uran.ua

Login to update | RIPEstat

```
inetnum:        77.47.133.0 - 77.47.133.255
netname:        NTUU-KPI-NET
descr:          National Technical University of Ukraine
descr:          "Kiev Polytechnic Institute"
descr:          Virtual Hosts Network
country:        UA
admin-c:        KPI-RIPE
tech-c:         KPI-RIPE
status:         ASSIGNED PA
mnt-by:         KPI-MNT
created:        2012-12-15T23:02:37Z
last-modified:  2012-12-15T23:02:37Z
source:         RIPE
```

7-уровневая модель OSI

Тип данных	Уровень (layer)	Функции
Данные	7. Прикладной (application)	Доступ к сетевым службам
	6. Представительский (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

5-й уровень модели OSI

Управление сеансом связи

5-й (сеансовый) уровень сетевой модели OSI отвечает за поддержание сеанса связи, позволяя взаимодействовать между собой различным приложениям, работающим одновременно.

Основные функции сеансового уровня:

- создание/завершение сеанса;
- поддержание сеанса связи, в том числе в периоды неактивности приложений, позволяя приложениям взаимодействовать между собой длительное время;
- синхронизация задач;
- управление правом на передачу данных.

5-й (сеансовый) уровень

Пример:

Видеоконференция в сети, когда звуковой поток
(с микрофона одного компьютера на динамик другого)
и видеопоток (с видеокамеры одного на экран другого)
синхронизируются для синхронизации движения губ с речью.

Синхронизация передачи обеспечивается помещением
в потоки данных контрольных точек (меток).

Управление правами на участие в разговоре гарантирует,
что именно тот человек, который показывается на экране,
действительно является тем, кто говорит в этот момент.

Резюме

5-й (сеансовый) уровень модели OSI

Фактически в установлении, поддержании и завершении сеансов в той или иной степени участвуют и протоколы других уровней (напр. TCP-протокол решает подобную задачу для потока данных при пересылке файла).

5-й (сеансовый) уровень позволяет правильно комбинировать или синхронизировать информацию **разных** потоков, возможно, происходящих из разных источников.

5-й (сеансовый) уровень

- https://ru.wikipedia.org/wiki/Сеансовый_уровень
- https://ru.qaz.wiki/wiki/Session_layer
- https://it-black.ru/funktsii-verkhnikh-urovney-setevoy-modeli/
- https://studme.org/94312/informatika/seansovyy_uroven_session_layer