

CENTER FOR MONITORING AND CONTROL OF THE
PUBLIC SERVICES TELECOMMUNICATION NETWORK
(CMC PSTN)

National Domain Name System (NDNS)
Instructions for Telecommunication Operators and AS number owners

Table of Contents

1. General information	3
2. Order of actions	3
3. Addresses and names of the NDNS public resolvers	3
4. NDNS configuration for Operator's public resolvers	4
5. Configuration for authoritative root zone server	4

1. General information

National Domain Name System (NDNS) is a union of interconnected software and hardware agents intended for storage and retrieval of information about network addresses and domain names.

NDNS is carried out by telecommunication operators, owners of any other operators of technology networks with autonomous system numbers, information publishers on the Internet, users of telecommunication services, or other parties requiring information contained in NDNS.

For usage of the public servers (resolvers) of the NDNS, owners of an autonomous system number **must change and/or add addresses** of the NDNS resolvers to the list of end user DNS servers (including the addition of those addresses to the DHCP configuration).

IMPORTANT! Backup current configuration before changing DNS configuration for NDNS usage to be able to roll back any time.

2. Order of actions

- 2.1. Study this instruction;
- 2.2. Perform configuration of the telecommunication operator (AS owner) following this instruction;
- 2.3. Send a notification about performed configuration to the regional Office of Roskomnadzor and to the CMC PSTN e-mail - ndr@noc.gov.ru.

Notification should contain full organization name (or natural person, or business name), Individual Taxpayer Number, regional location and contacts of a person responsible for provisioning configuration. In the notification, include subject "Connection to the NDNS", short name, Individual Taxpayer Number should be mentioned, for example: «Connection to the NDNS_Spring llc_1111111111» or «Connection to the NDNS_V.V. Ivanov_111111111122».

3. Addresses and names of the NDNS public resolvers

	<i>a.res-nsdi.ru</i>	<i>b.res-nsdi.ru</i>
ipv4	195.208.4.1	195.208.5.1
ipv6	2a0c:a9c7:9::1	2a0c:a9c7:8::1

Any of these addresses may be used as primary or secondary DNS server.

4. Configuration settings for using the public NDNS resolvers

For configuration of the caching DNS resolvers autonomous system number owner must modify configuration to receive answers from local authoritative root zone server:

for **BIND 9.11** DNS resolver

```
options {
  forward first;
  forwarders { 195.208.4.1; 195.208.5.1; 2a0c:a9c7:8::1;
              2a0c:a9c7:9::1;};
};
```

for **Unbound** DNS resolver

```
forward-zone:
  name: "."
  forward-host: 195.208.4.1
  forward-host: 195.208.5.1
  forward-host: 2a0c:a9c7:8::1
  forward-host: 2a0c:a9c7:9::1
  forward-first: yes
```

for **PowerDNS-recursor** DNS resolver

```
forward-zones=.= 195.208.4.1;195.208.5.1;2a0c:a9c7:8::1;2a0c:a9c7:9::1
```

5. Configuration for authoritative root zone server

For configuration of the local authoritative server to support root zone received from the distribution server autonomous system number owner must:

- Copy zone file (tab «Zone file» → selection «--zone serial number-- » → button «Show» →button «Download file»);
- Change configuration of the local DNS server:

in case of local DNS server is **BIND 9.11**

```
options {
  ...
  listen-on {127.0.0.1; <external address for notifications>;};
  ...
}
```

```
key "<keyname>" {
  algorithm hmac-sha256;
  secret "<secret>";
```

```

};
server 194.85.254.37 { keys { <keyname> }; };
    zone "." {
        type slave;
        file "<path/to/file>";
        masters { 194.85.254.37; };
    };
};
in case of local DNS server is NSD
    ip-address: 127.0.0.1
    ip-address: <external address for notifications>

    key:
        name: "<keyname>"
        algorithm: hmac-sha256
        secret: "<secret>"
    zone:
        name: "."
        zonefile: "<path/to/file>"
        allow-notify: 194.85.254.37 <keyname>
        request-xfr: 194.85.254.37 <keyname>

```

<external address for notifications>

– IP address of the server, which will receive updates of the root zone updates at the master server (value must be the same with «IP address of your server» at the page «AXFR configuration»)

<keyname> – value «Key Title» (tab «AXFR configuration»)

<secret> – value «Key» (tab «AXFR configuration»)

<path/to/file> – path to the root zone file

Important! To let DNS server **NSD** to function as DNS root server it is required to set compilation option **--enable-root-server**, otherwise NSD will not load the root zone file.

ЦЕНТР МОНИТОРИНГА И УПРАВЛЕНИЯ
СЕТЬЮ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

**Инструкция по подключению операторов связи и владельцев АС к
Национальной системе доменных имен (НСДИ)**

Оглавление

1. Общие сведения	3
2. Порядок действий	3
3. Адреса и имена публичных резолверов НСДИ	3
4. Настройки для использования публичных резолверов НСДИ.....	4
5. Настройки для использования авторитетного сервера корневой зоны	4

1. Общие сведения

Национальная система доменных имен (НСДИ) представляет собой совокупность взаимосвязанных программных и технических средств, предназначенных для хранения и получения информации о сетевых адресах и доменных именах.

Использование НСДИ осуществляется имеющими номер автономной системы операторами связи, собственниками или иными владельцами технологических сетей связи, организаторами распространения информации в сети "Интернет", пользователями услугами связи, а также иными лицами, которым необходимы сведения, содержащиеся в национальной системе доменных имен.

Для использования публичных серверов (резолверов) НСДИ владельцу автономной системы необходимо изменить и/или добавить в список DNS-серверов для конечного клиента адреса резолверов НСДИ (необходимо внести адреса этих серверов в настройки DHCP).

ВАЖНО! Прежде чем изменять настройки DNS для использования серверов НСДИ, **обязательно сохраните текущие настройки в качестве резервных копий на случай, если понадобится вернуться к ним в любое время.**

2. Порядок действий

- 2.1. Изучить данную инструкцию;
- 2.2. Выполнить настройки, согласно инструкции, на оборудовании оператора связи (владельца АС);
- 2.3. Направить уведомление о выполненных настройках в территориальное Управление Роскомнадзора и на электронную почту ЦМУ ССОП - ndr@noc.gov.ru.

В уведомлении указать полное название организации (или физического лица, ИП), ИНН, регион местонахождения и контакты лица ответственного за произведенные настройки. В названии уведомления необходимо указать: Подключение к НСДИ, краткое название организации и ИНН, например: «Подключение к НСДИ_ООО «ВЕСНА»_1111111111» или «Подключение к НСДИ_ИП В.В.ИВАНОВ_11111111122».

3. Адреса и имена публичных резолверов НСДИ

	<i>a.res-nsdi.ru</i>	<i>b.res-nsdi.ru</i>
ipv4	195.208.4.1	195.208.5.1
ipv6	2a0c:a9c7:9::1	2a0c:a9c7:8::1

Любой из указанных адресов может быть использован в качестве основного или дополнительного DNS-сервера.

4. Настройки для использования публичных резолверов НСДИ

Для настройки кэширующих DNS-резолверов на получение ответов от локального авторитетного сервера корневой зоны владельцу автономной системы необходимо внести изменения в конфигурационные файлы DNS-резолверов:

- если реализация DNS-резолвера **BIND 9.11**

```
options {
    forward first;
    forwarders { 195.208.4.1; 195.208.5.1; 2a0c:a9c7:8::1;
                2a0c:a9c7:9::1;};
};
```

- если реализация DNS-резолвера **Unbound**

```
forward-zone:
    name: "."
    forward-host: 195.208.4.1
    forward-host: 195.208.5.1
    forward-host: 2a0c:a9c7:8::1
    forward-host: 2a0c:a9c7:9::1
    forward-first: yes
```

- если реализация DNS-резолвера **PowerDNS-recursor**

```
forward-zones=. = 195.208.4.1;195.208.5.1;2a0c:a9c7:8::1;2a0c:a9c7:9::1
```

5. Настройки для использования авторитетного сервера корневой зоны

Для настройки локального авторитетного сервера для поддержки на нем корневой зоны, полученной с сервера дистрибуции, владельцу автономной системы необходимо:

- Скопировать файл зоны (вкладка «Файлы зоны» → выбор «--серийный номер зоны--» → кнопка «Показать» → кнопка «Скачать файл»);
- Внести изменения в конфигурационные файлы локального DNS -сервера:

- если реализация локального DNS-сервера **BIND 9.11**

```
options {
    ...
    listen-on {127.0.0.1; <внешний адрес для уведомлений>;};
    ...
}
```

```

key "<keyname>" {
    algorithm hmac-sha256;
    secret "<secret>";
};
server 194.85.254.37 { keys { <keyname> }; };
zone "." {
    type slave;
    file "<path/to/file>";
    masters { 194.85.254.37; };
};

```

- если реализация локального DNS-сервера **NSD**

```

ip-address: 127.0.0.1
ip-address: <внешний адрес для уведомлений>

```

```

key:
    name: "<keyname>"
    algorithm: hmac-sha256
    secret: "<secret>"
zone:
    name: "."
    zonefile: "<path/to/file>"
    allow-notify: 194.85.254.37 <keyname>
    request-xfr: 194.85.254.37 <keyname>

```

<внешний адрес для уведомлений>	– IP-адрес сервера, на который будут приходить уведомления об обновлении корневой зоны на master-сервере (значение должно совпадать с указанным в поле «IP-адрес вашего сервера» на странице «AXFR настройки»)
<keyname>	– значение «Название ключа» (вкладка «AXFR настройки»)
<secret>	– значение «Ключ» (вкладка «AXFR настройки»)
<path/to/file>	– путь к файлу корневой зоны

Важно! Для функционирования DNS-сервера **NSD** в качестве сервера корневой зоны DNS при компиляции необходимо установить флаг **--enable-root-server**, в противном случае NSD не будет загружать файлы корневой зоны.