APNIC

Afghanistan, American Samoa, Australia, Bangladesh, Bhutan, British Indian Ocean Territory, Brunei Darussalam, Cambodia, China, Christmas Island, Cocos Keeling Islands, Cook Islands, East Timor, Fiji, French Polynesia, French Southern Territories, Guam, Hong Kong, India, Indonesia, Japan, Kiribati, North Korea, South Korea, Laos, Macau, Malaysia, Maldives, Marshall Islands, Micronesia, Mongolia, Myanmar, Nauru, Nepal, New Caledonia, New Zealand, Niue, Norfolk Island, Northern Mariana Islands, Pakistan, Palau, Papua New Guinea, Philippines, Pitcairn, Samoa, Singapore, Solomon Islands, Sri Lanka, Taiwan, Thailand, Tokelau, Tonga, Tuvalu, Vanuatu, Vietnam, Wallis and Futuna Islands.

Reverse DNS Delegations

Addressing the challenge of responsible Internet resource distribution in the Asia Pacific region

Asia Pacific Network Information Centre

Table of contents

Reverse DNS Delegations

The Domain Name System (DNS) is a globally distributed Internet service. Among other services, it provides name-to-number (forward) and number-to-name (reverse) translations, using defined client-server and server-server protocols. The DNS is a public service and any user is freely able to query the DNS system for forward or reverse translations.

Reverse DNS delegations allow requestors to map to a domain name from an IP address. Reverse delegation is achieved by the use of pseudo-domain names in-addr.arpa (IPv4) and ip6.arpa (IPv6).

APNIC only registers reverse delegations and is not directly involved in other aspects of the domain name registration system.

Public availability of reverse DNS zones at APNIC

For all IP address blocks IANA (Internet Assigned Numbers Authority) allocates to APNIC, IANA also delegates corresponding reverse DNS zones within the centrally administered "in-addr.arpa" and "ip6.arpa" domains. The lists of DNS zones currently maintained by APNIC are available at:

http://www.apnic.net/info/reports/index.htm (IANA data).

APNIC also published zone fragments. Zone fragments are the parts of zones managed by other parties, namely:

- The other RIRs (Regional Internet Registries), who share zone management of early registration networks
- The NIRs (National Internet Registries), who manage IP address space allocated to them for further distribution to their members

Access to reverse DNS data

Apart from access via conventional DNS query, APNIC supports access to reverse DNS data in four ways:

1. Whois queries, either directly to APNIC from other whois services or via the Web
2. Bulk access to the APNIC Whois Database by FTP or NRTM (Near Real Time Mirroring)
3. FTP access to the DNS zone files
4. DNS zone transfer queries

Operational and policy restrictions are imposed on data access via each of these methods. These restrictions are in place to protect the performance of the systems being used to provide DNS services and to limit 'mining' and misuse of administrative data (such as contact records).

Access to reverse DNS data by whois query

The APNIC Whois Database is currently used as the management database for producing the DNS zones so it can provide the information for each delegated IPv4 and IPv6 range registered in the reverse DNS.

Outside the global DNS system, information regarding reverse DNS delegations can be checked via whois queries.

The information is stored as domain objects (RPSL format). The name of each domain object is the reverse DNS zone under in-addr.arpa or ip6.arpa. The "nserver" attributes in each domain object define the officially-delegated DNS nameservers (the NS in DNS) zone contents. To see what a completed domain object looks like, you can view an example at:

http://www.apnic.net/db/ref/examples/domain.html

Ordinary access via whois queries is subject to daily limits. Queries via the web-based whois interface are also subject to rate-based limits.These access limits apply to all the whois data, not just that which is DNS related. The actual limits set are monitored by the APNIC Secretariat and adjusted where appropriate.

Access to reverse DNS data by FTP

APNIC publishes the DNS zone information as text files at:

ftp://ftp.apnic.net/pub/zones

The files are published with an associated file with the zones' MD5 checksum and a detached PGP signature so they can be verified independently.

There are no Acceptable Use Policy (AUP) restrictions on general access to the APNIC FTP service, but APNIC reserves the right to limit the simultaneous connections, the number of downloaded files, and the total data size downloaded per connection to limit the load on the servers and the network.

Access to reverse DNS by zone query

Visibility of the data via DNS zone transfer (AXFR and IXFR) may be limited to listed secondary DNS nameservers only.

Attributes of reverse delegation (domain) objects

Reverse delegation template

To view the reverse delegation (domain) template, see the APNIC Whois Database object templates, see:

http://www.apnic.net/db/ref/object-templates.html#inetnum.

Reverse delegation attributes

The mandatory and optional attributes in the reverse delegation domain object are:

Mandatory attributes

Attribute	Description
domain	The name of the reverse delegation. For IPv4 reverse delegation, use the format x.x.x.x.in-addr.arpa. For example: • 181.137.202.in-addr.arpa • 137.202.in-addr.arpa For IPv6 reverse delegations, use the format x.x.x.x.ip6.arpa.
descr	The name of the organization responsible for the reverse delegation. It also can describe the use of the IP range in the domain object. For example: • Reverse delegation for ExampleNet-WF • Reverse delegation for 202.137.181.0/20 • Reverse delegation for Sparkynet customer
admin-c	The NIC-handle of an onsite contact person or role object.There may be more than one admin-c listed. In the web interface, the admin-c field contains a link to the person or role object the NIC-handle belongs to.

Attribute	Description
tech-c	The NIC-handle of a technical contact person or role object. There may be more than one tech-c listed. In the web interface, the tech-c field contains a link to the person or role object the NIC-handle belongs to.
zone-c	The NIC-handle of a person or role object with authority over a zone. There may be more than one zone-c listed. In the web interface, the zone-c attribute contains a link to the person or role object the NIC-handle belongs to.
mnt-by	The identifier of a registered mntner object used for authorization and authentication of changes to the domain object. In the web interface, the mnt-by attribute contains a link to the specified mntner.
changed	The email address of who last updated the database object and the date it occurred.
source	The name of the database from which the data was obtained.

Optional fields

Attribute	Description
country	Two letter ISO 3166 (http://www.apnic.net/info/reference/lookup_codes.html) code of the country or economy where the admin-c is based.
sub-dom	This attribute is not applicable to reverse domains. Do not use this attribute. The APNIC Whois Database uses RIPE v3 database software. Some functions and options in RIPE software are not applicable to the APNIC Whois Database.
dom-net	This attribute is not applicable to reverse domains. Do not use this attribute. The APNIC Whois Database uses RIPE v3 database software. Some functions and options in RIPE software are not applicable to the APNIC Whois Database.
remarks	General remarks. May include a URL or email address.
notify	The email address to which notifications of changes to an object should be sent. The notify attribute is not to be used as a contact point for the organization responsible for the reverse domain.
mnt-lower	The identifier of a registered mntner object used to authorize the creation of reverse domain objects more specific that the reverse domain specified by this object.
refer	This attribute is not applicable to reverse domains. Do not use this attribute.

Registering your Reverse Delegations with APNIC

IMPORTANT

Before filling out this form, ensure that the zone has been loaded on your nameserver and associated secondaries. The diagnostic script uses both UDP and TCP to verify the nameservers, which may cause timeouts if you block TCP port 53.

In the case of /16 (slash sixteen) level delegations (that is, in-addr.arpa rather than /24 delegations, X.X.X.in-addr.arpa) APNIC can secondary the zone from your name servers in order to increase the visibility of your reverse delegations if required. Contact helpdesk@apnic.net for further information.

View, modify, or delete an existing domain object

To view, modify, or delete an existing domain object, view the following form:

For example: 123.153.203.in-addr.arpa

- http://www.apnic.net/apnic-bin/creform.pl

Create a new domain object

This form http://www.apnic.net/apnic-bin/creform.pl (or via ftp: ftp://ftp.apnic.net/apnic/docs/reverse-dns) allows you to create a new domain object. The appropriate in-addr-arpa or ip6.int zone must first be available on your nameservers before continuing with this form. APNIC will only perform reverse delegations on the "." (dot) boundaries. If you have less than 255 IP addresses, please contact your upstream provider.

Guide to reverse zones

Tools exist to manage DNS:

- http://www.dns.net/dnsrd/tools.html

Creating a reverse zone

Creating a reverse zone is the same as creating any other zone file. The Start of Authority (SOA) record and initial NS (NameServer) records are the same as any normal zone. However, you will need to create additional PTR records.

The following information is based on creating reverse zones using BIND. The principles should be the same for other DNS software; however, the details are likely to be different. If you are not using BIND, please see the documentation for the software package you are using.

Start of Authority (SOA) record

The SOA record is the first record in a properly configured zone. It contains information about the zone in a string of fields. An SOA record tells the server to be authoritative for the zone. The SOA record takes the format:

```
<domain.name.>  IN  SOA  <hostname.domain.name.>  <mailbox.domain.name>
                                                 <serial-number>
                                                 <refresh>
                                                 <retry>
                                                 <expire>
                                                 <minimum-ttl>
```

Where:

Field	Description
domain.name	The name of the domain to which the SOA belongs. Instead of writing out the full domain, you can also use '@' in the file to let the nameserver fill this out automatically. Example: • 28.12.202.in-addr.arpa • @
IN	The class of the DNS record. 'IN' is an abbreviated form of 'Internet'.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SOA</td><td>The type of DNS record, which in this case is ‘Start of Authority’.</td></tr>
<tr><td>hostname.domain.name</td><td>Also known as the ‘master’ field. It contains the hostname of the primary zone server. This indicates the machine on which changes to the zone file should be made.</td></tr>
<tr><td>mailbox.domain.name</td><td>Also known as the ‘hostmaster’ field. It contains the e-mail address of the person responsible for maintaining the zone. No ‘@’ is used as this field was originally formatted as if it were a hostname (in which ‘@’ was invalid). The ‘@’ symbol is replaced by a ‘.’, and any ‘.’ before the “@” was replaced by ‘\’. Examples:
<table>
<tr><th>email address:</th><th>hostmaster field</th></tr>
<tr><td>helpdesk@apnic.net</td><td>helpdesk@apnic.apnic.net</td></tr>
<tr><td>dns.admin@apnic.net</td><td>dns\admin.apnic.net</td></tr>
</table>
Recently, arbitrary characters have been permitted in this field, so ‘@’ can now be used. However, the old format is still used by the majority of hostmasters and it is assumed by many DNS validators.</td></tr>
<tr><td>serial number</td><td>The serial number of the current version of the DNS database for this domain. If a secondary server’s number is lower than the number of the primary server, it indicates that the secondary server’s records are out of date and that it requires a zone transfer from the primary server.</td></tr>
<tr><td>refresh</td><td>This tells a secondary server how often to poll the primary server and check for changes in the serial number field. This is measured in seconds.</td></tr>
<tr><td>retry</td><td>If a refresh attempt fails a secondary server will retry after the interval specified in the retry field. This is measured in seconds.</td></tr>
<tr><td>expire</td><td>If the refresh and retry attempts fail, the secondary server will stop serving the zone after the period specified in the expire field. This is measured in seconds.</td></tr>
<tr><td>minimum-ttl</td><td>The default TTL (Time To Live) for every record in the zone. The default is only used when a particular resource record does not have its own specified TTL value. When changes are being made to a zone, the default is often set at ten minutes or less.</td></tr>
</table>

Example of an SOA record:

```
28.12.202.in-addr.arpa.   IN SOA   ns.apnic.net.   helpdesk@apnic.net. (
                                                        1999040701  ;Serial number
                                                        10800       ;Refresh
                                                        3600        ;Retry
                                                        604800      ;Expire
                                                        86400)      ;Minimum TTL
```

The “;” character in the example above indicates that the rest of the line is a comment that should be ignored by the nameserver. Also note: The trailing dot (“.”) after each record refers to a hostname. Without the dot, the nameserver adds the current zone after the record. For example, ns.pnic.net would be interpreted as ns.apnic.net.28.12.202.in-addr.arpa.

Nameserver (NS) records

An NS record declares the nameservers that serve a given zone. The NS record takes the format:

<domain.name> IN NS <hostname.dmain.name>

Where:

Field	Description
domain.name	The name of the domain to which the NS belongs. Instead of writing out the full domain, you can use "@" in the file to let the nameserver fill this out automatically. For example: • 28.12.202.in-addr.arpa • @ • [space]
IN	The class of the DNS record. "IN" is an abbreviated form of "Internet".
NS	The type of DNS record, which in this case is "Nameserver".
hostname.domain.name	The hostname of an authoritative server.

Example NS record:

- IN NS ns.apnic.net.
- IN NS svc00.apnic.net.
- IN NS ns.telstra.net.
- IN NS rs.arin.net.

Pointer (PTR) records

Within the zone, you then need to create domain pointer (PTR) records for each IP address.

For the address "202.12.28.131" this would be:

131.28.12.202.in-addr.arpa. IN PTR svc00.apnic.net.

However, as the SOA record for the zone already states the in-addr.arpa domain in full, you do not need to write this out again. Instead, you need only write the last dotted quad from the address. Therefore, the above PTR entry can also be written as follows:

131 IN PTR svc00.apnic.net.

Once you have created all the relevant PTR records for your in-addr.arpa zone, the next step is to load it onto your nameserver.

Nameserver software

There are various implementations of DNS protocols. The most popular is BIND (Berkeley Internet Name Domain). Information is available on the latest version of Bind at:

- ISC BIND (https://www.isc.org/bind.html)

APNIC recommends that you install BIND 9 as this version has more features and security fixes than previous versions.

A list of other DNS nameserver software is available at:

- http://www.dns.net/dnsrd/servers.html

Using BIND 9 to set up the primary nameserver for a zone.

1. Add an entry specifying the primary server to the named.conf file using the following format:

```
zone "<domain-name>" in {
        type master;
        file "<path-name>";
};
```

Where:

Field	Description
domain-name	The name of the domain. For example: • 28.12.202.in-addr.arpa.
type-master	Defines the nameserver as the primary nameserver for <domain-name>.
path-name	The location of the file that contains the zone records. The name of the file is entirely arbitrary. What you many choose to name the file has no relationship to the name of the zone that is being made primary. If you have a large site, consider using the "include" command to avoid an excessively large named.conf:

2. Tell the nameserver to read in the new zone file by executing the command:

```
rndc reconfig
```

3. Example primary nameserver:

```
zone "28.12.202.in-addr.arpa" in {
    type master;
    file "reverse/28.12.202.in-addr.arpa";
};
```

Using BIND to set up a secondary nameserver for a zone

1. Add an entry specifying the secondary server to the named.conf file using the following format. For example:

```
zone "<domain-name>" {
    type slave;
    file "path-name";
    masters {
    <ip-address>;
    };
};
```

Where:

Field	Description
<domain-name>	The name of the domain. For example: • 28.12.202.in-addr.arpa
type slave	Defines this server as a secondary name server.
path-name	The location of the file that contains the zone records. The name of he file is entirely arbitrary. What you may choose to name the file has no relationship to the name of the zone that is being made secondary.
masters	Refers to the location of the primary of master nameserver
<ip-address>	The IP address of the primary nameserver.

2. Tell the nameserver to reconfig using the command:

```
rdnc redonfig
```

Example of a secondary nameserver:

```
zone "28.12.202.in-addr.arpa" {
    type slave;
    file "slave/28.12.202.in-addr.arpa";
    masters {
    203.37.255.97;
    };
};
```

Deprecation of ip6.int for reverse DNS delegations

From 1 June 2006, APNIC deprecated all ip6.int reverse delegation services resulting in holders of IPv6 space creating reverse domain objects using ip6.arpa.

Troubleshooting for Reverse Delegations

Common errors

My domain object is in the database but it isn't visible to the Internet.

The authoritative nameserver, ns.apnic.net is reloaded every two hours. Updates should become visible at the next nameserver reload.

If your domain is still not visible more than two hours after you have successfully created a domain object, please contact the APNIC Helpdesk (helpdesk@apnic.net).

I don't have a maintainer object. How can I request a reverse delegation domain object?

Request a maintainer object via the appropriate web form (http://www.apnic.net/apnic-bin/maintainer.pl). Maintainer objects are used to protect a given object in the APNIC database from ad-hoc changes. As such, APNIC staff can only create them.

What does "hierarchical authorization failed, request forwarded to maintainer" mean?

Another use of maintainer objects is to protect the space that is logically beneath an object with the mnt-lower attribute set. There exists a domain object named in-addr.arpa, which has the mnt-lower set, which ensures that no unauthorized creations occur beneath the in-addr.arpa zone.

If you request the creation of a new in-addr.arpa domain, it will usually fail the hierarchical authorization, producing an automatic email reply. This reply will also be automatically forwarded to the APNIC helpdesk staff, who will create the new domain for you. An email notification will be sent out when the new domain has been created. This only occurs on initial creation, and should not occur when you wish to update the delegation (as it will be maintained by your own maintainer object).

Please do not confuse this error message with the standard "authorization failed" message (which indicates that you have supplied the wrong password for the specified maintainer object).

ERROR: must specify at least "2" separate nservers

You are required to provide at least two functional nameservers to create a reverse domain.

ERROR: No SOA RR were found

No Start of Authority (SOA) records were found. This tends to indicate that the nominated nameservers are not replying correctly for the zone in question. Usually, you can fix this by reloading all of the nameservers.

WARNING: some of the specified name servers appear to be in the same subnet; according to RFC2182 they should be geographically separated.

If you supply more than one nameserver that appears to be in the same physical location, you may get this warning as a reminder that the zone may not be visible if your connection to the Internet fails. Having off-site secondary nameservers can be considered a form of insurance for system failure, for example, fire in your machine room.

APNIC highly recommends that you have multiple secondary nameservers located outside your network to cover system or network failures.

ERROR: NS RR for abc.b.c.d found on xyz.b.c.d but not in template.

The machine abc.b.c.d is reported to be a nameserver for this domain by the machine xyz.b.c.d, but you did not list abc.b.c.d when submitting the form.

ERROR: nserver: a.b.c.d

ERROR: The specified name server is not responding

The nameserver a.b.c.d has failed to respond because:

- A nameserver process is not running on port 53

or

- The nameserver does not accept both UDP and TCP port 53 queries

or

- The nameserver process is running on the given host but has not been loaded with information about itself

Correct your nameserver or firewall/router configuration and resubmit the request.

ERROR: cross-check of listed NS RR failed.

The nameservers on both zones should be the same.

ERROR: SOA on "machine1.b.c.d" does not match SOA on "machine2.b.c.d"

Some of the nameservers supplied could not be contacted or some of them failed to respond appropriately, that is, is a nameserver running on these hosts and do they know about the zone in question?

This message is also gnenerated when a list of nameservers that you supply to the form does not match the list of nameservers that you set up (on the nameservers in question). The comparisons are done on a textual basis, that is, supplying IP addresses won't work.

Help, I'm sure my zone is set up correctly but your form just won't accept it

You can always email helpdesk@apnic.net for help. However, we suggest that you first read RFC1912 – Common DNS Operational and Configuration Errors (http://www.ietf.org/rfc/rfc1912.txt).

Revision	Date	Version	Comment
1	8 April 2009	1.0	

www.apnic.net

APNIC

Asia Pacific Network Information Centre
APNIC Pty Ltd
ABN: 42 081 528 010

6 Cordelia Street
PO Box 3646
South Brisbane
QLD 4101 AUSTRALIA

URL www.apnic.net
SIP apnic@voip.apnic.net

Phone +61 7 3858 3100
Fax + 61 7 3858 3199