

---

# Guidelines for Operation of DNS Infrastructure by ccTLDs

---

Asia Pacific Top Level  
Domain Association

---

August 2007

---



# Guidelines for Operation of DNS Infrastructure by ccTLDs

## Background

APTLD is the association of Country Code Top Level Domain operators in the Asia-Pacific Region. More information about our work can be found at [www.aptd.org](http://www.aptd.org).

This paper, based on work done by Chris Wright and Adrian Kinderis of AusRegistry, provides Guidelines for Operation of DNS Infrastructure by ccTLDs.

## Introduction

The Internet is rapidly becoming more and more popular, broadband adoption is increasing, and the Internet is becoming a major focus of government and industry bodies. Governments, Businesses and the local and global Internet communities are calling for greater accountability and responsibility to be taken by those organisations responsible for running and maintaining the DNS infrastructure.

The importance of the Internet in everyday life is ever increasing for commerce, share trading, Internet banking, bills, information and research, education, collaboration and entertainment. There are not many industries remaining where the Internet does not have some impact. The Internet is used on a daily basis by many people, including government, to conduct business, and communicate.

Due to this, the security and stability of the Internet, of which DNS is a major component, is becoming more and more of a concern to various government and industry bodies.

Arrangements that may have been put in place many years ago may have only evolved slightly, despite this rapid growth. These arrangements were fit for the time when the Internet was a flourishing

research network which had not established its place in a commercialised capacity. But now, as usage patterns of the Internet have changed, and the expectations and requirements of various organisations have changed an evolution of the way the DNS is operated and managed needs to take place.

Greater responsibilities are being required of Name Server Operators due to these changes in conditions. Some of these responsibilities Operators may not even be aware of; others are not enforceable due to the nature of the agreements (or lack thereof) under which they are providing services. As the new, primarily security oriented requirements increase, and combine with the increases in traffic volumes, resource requirements on Operators in turn increase. Volunteer Operators are reluctant to enter into formal arrangements and in fact many have already expressed their concerns, retracted offers for service and/or have indicated a desire to be "phased out". An example of such an organisation is RIPE NCC, which in its 'RIPE NCC Activity Plan 2007', published on December 20<sup>th</sup> 2006, stated that it will "cease providing secondary DNS name services for well-established ccTLDs" (<http://www.ripe.net/ripe/docs/ripe-398.html>).

The scope and scale of the way that DNS Services are provided will depend on the topology chosen, the implications of failure, and possibility of attack. It will also depend on the policies, technologies and funds that a ccTLD has.

## Requirements of DNS Services

The following is a list of guidelines any ccTLD should be striving to achieve. These requirements may require further research, analysis and refining depending on individual circumstances, however they provide a strong basis to build on. These requirements have been drawn from RFCs, Internet Standards, the experience of Registry Operators and other industry participants.

The relevant RFCs and Standards can be found on the RFC Editor website and the IETF website at:

- [www.rfc-editor.org/](http://www.rfc-editor.org/)

- [www.ietf.org/](http://www.ietf.org/)

## The DNS Service

The DNS Service is defined as the overall ability to locate an authoritative resource record within a zone or domain within the namespace. The collection of all Name Services that provide DNS resolution services for the namespace make up this overall DNS Service.

The DNS service:

MUST...	SHOULD...
...be designed in such a way that temporary losses of a significant number of the Name Servers SHOULD NOT affect the operation of the Internet.	...be scalable to meet future demands.
...be supplied by multiple Name Services. There should be at least two, but not so many that keeping them in synch becomes a burden.	...comprise at least 5 Name Services that consist of Name Servers which are independent of the other Name Services.
...consider the values used in the SOA of each zone and need to select appropriate values for the usage style of the zone with clear logical reasoning behind decisions. These should be researched and documented.	...publish the appropriate SRV and NAPTR records for WHOIS and Registration services
...not be the sole responsibility of one DNS provider.	...make use of a “stealth primary” server to distribute updates to the publicly queryable Name Servers. A stealth primary is a name server that is inaccessible to the public.

...ensure that Name Services are provided with Geographic diversity in mind. The selection of sites should be based on the source of queries so that network impacts and delays can be minimised.	... whilst unusual configurations involving multiple primary servers are possible, these can result in data inconsistencies and SHOULD be avoided.
...ensure that Network topological diversity is maintained by Name Services.	...ensure that technologies such as DNSSEC are properly evaluated and if appropriate ensure consistent support for these technologies across all Name Services.
...ensure that reasonable methods of enhancing reliability and performance are employed given resource restrictions.	...have all Name Services published with a consistent domain (to take advantage of DNS packet compression) and be GLUED at the root-server level where appropriate.
... ensure that management traffic is cryptographically secured.	...ensure that a diversity of DNS Software, Operating System, Architectures, and Networking Equipment etc is used to provide the service. Managed diversity enhances robustness.

...note that while zone file updates do not need to be encrypted, they must be cryptographically signed (e.g. TSIG) to ensure that the updates are correct and sourced from the correct server.

A Name Server Operator concerned about zone contents being intercepted while in transit may wish to encrypt these as well.

## Name Service

A collection of Name Servers, that may or may not necessarily be located at the same Name Server Site, which respond to the same IPv4 and/or IPv6 address for the purpose of answering DNS queries are said to be providing a "Name Service". For example these may be a number of servers load balanced together at a single site, or the broader AnyCast instance of a group of single Name Services. These addresses are typically published as the authoritative servers.

Name Services:

- Should consist of a number of individual Name Servers.
- Should be capable of processing 10 times the peak transactions per second (tx/s) load experienced by any Name Service under normal operating conditions. This is to allow headroom to mitigate Distributed Denial of Service attacks and to handle load increases should failure of other Name Services occur. The fewer overall Name Server (Network) sites that are available the greater the headroom capacity should be allowed.
- Should have sufficient bandwidth available to satisfy the above target transaction loads.

- Should answer any valid query from any valid IP address.
- Should not answer AXFR or other zone transfer queries from clients other than an identified list of the ccTLD's Name Servers.
- Should have their IPv4 (in-addr.arpa) and IPv6 equivalent reverse resolution records appropriately configured.
- Should terminate access via both IPv4 and IPv6 transport, at this stage of IPv6 deployment it is acceptable for the IPv6 transport to be tunnelled in from an external party, HOWEVER all security concerns are still to be considered.
- Must not only be accessible via IPv6.

## Name Server

An individual server that is responsible for providing DNS resolution services is a "Name Server".

Name Servers Must...

- ... use DNS software which is fully compliant with IETF standards for DNS. The relevant RFCs and Standards can be found on the RFC Editor website and the IETF website at:
  - [www.rfc-editor.org/](http://www.rfc-editor.org/)
  - [www.ietf.org/](http://www.ietf.org/)
- ... provide authoritative responses ONLY for the zones they serve.
- ... have recursive lookups disabled.
- ... have DNS forwarding disabled.
- ...should block bogon IP addresses
- ...configured securely following the well known online examples such as the Ssecure BIND Template ([www.cymru.com](http://www.cymru.com)).

- ... have any mechanism which can cause it to “cache” or return a “cached” result disabled.
- ... generate UDP checksums when sending UDP datagrams and ... verify checksums when receiving UDP datagrams containing a non-zero checksum.
- ... be used EXCLUSIVELY for providing name resolution services for ccTLDs, gTLDs and associated zones only. It should not be used for general DNS hosting.
- ... be used EXCLUSIVELY for the purposes of providing DNS services only.
- ... have their clocks synchronised via the Network Time Protocol (NTP).
- ... NOT be configured to be NTP servers.
- ... log all logins and login attempts these logs ... be audited regularly by the Operator.
- ... have their IPv4 (in-addr.arpa) and IPv6 equivalent reverse resolution records appropriately configured.
- ... be DNSSEC capable
- ... support IPv4 and IPv6
- They should perform all logging with GMT time stamps.

## Name Server Site

A site or more specifically the area within a site that is used to house Name Servers is referred to as the “Name Server Site.”

Name Server Sites should:

- ...house multiple Name Servers (at least 2, with more only being required if 2 cannot handle transaction loads), these Name Servers should be load balanced and must NOT be listed as individual Name Services.
- ...support the ability for any Internet provider to directly connect to the network at their OWN expense.
- ...have physical security which is in a manner expected of data centres critical to a major enterprise.
- ...have “positive access controls” meaning all individuals with access must be identified, limited, controlled and logged.
- ...have Security personnel in attendance and be regularly patrolled.
- ...have 24 hour surveillance systems.
- ...be physically protected by lock and key.
- ...have Redundant Power abilities including the ability to continue to supply power for at least 24 hours after total mains power supply failure.
- ...have Fire Detection and/or suppression systems.
- ...have continuity of service mechanisms similar to those expected for critical infrastructure in a major enterprise.
- ...use multiple redundant Internet Feeds.
- ...have an N+1 redundancy on ALL critical path devices and services.
- ...organise Name Servers in such a manner that automatic failover and isolation of a malfunction server occurs and continuity of

service is maintained. This should include the removal of AnyCast routes if all Name Servers at a site fail.

- ...have spare equipment on standby.
- ...have appropriate support contracts in place with suppliers to ensure timely resolution of failures.
- ...ensure that ONLY Name Servers and their supporting infrastructure are connected to the Network.
- ...implement appropriate Traffic Filtering and shaping policies.
- ...ensure that all logging is duplicated to a separate server suitably protected.
- ...deploy Network Intrusion Detection mechanisms.
- ...be protected from attacks based on source routing.
- ...use secure remote administration methods accessible only from known administration points (encrypted and authenticated). IPSEC is considered mandatory.
- ...if capable implement source IP verification techniques, such as those offered by vendors like Cisco (Unicast Reverse Path Verification).

## DNS Providers & Operators

An organisation that manages one or more “Name Service” is a “DNS provider”. The employees within that organisation that manage and maintain the “Name Service” and its associated equipment are the “DNS Operators”.

Providers should:

- ...at always have at least 2 Operators on staff.

- ...ensure that an Operator is available 24 hours a day, 7 days a week on a centralised contact number.
- ...ensure that any contact to the number is responded to within 30 mins and that priority to resolve problems is the highest possible within the organisation (where appropriate to the problem at hand).
- ...ensure that they meet all requirements of this documentation.
- ...follow all policies and procedures outlined by ccTLD Manager.
- ...notify the ccTLD Manager immediately as soon as any failure of DNS service or any changes in contact details etc are required.
- ...ensure that planned outages are communicated between providers and should ensure that only one site is undergoing maintenance at a time.

Operators should:

- ...have significant experience in operating iterative DNS services.
- ...be adequately trained and experience in the operation and maintenance of all equipment being used to provide the service.
- ...keep up to date with the latest developments and standards relating to DNS.
- ...be members of the DNS Operators mailing list.

## Monitoring, Logging & Statistics

Statistics are an important part of the DNS operation as it allows trends, increases, capacity planning and anomaly detection to be quickly and easily performed. Monitoring of service availability, performance and logs is important in detecting system failures, hacking attempt and various other attacks.

Statistics should...

- ...be kept by each DNS provider for each Name Server they operate
- ...be aggregated on a regular basis to a central location and a backup.
- ...be kept on metrics such as query counts, types, usage rates, loads, OS statistics, response times, outages etc.

Monitoring should:

- ...be performed by each DNS provider (detailed) for all Name Servers/Services they provide.
- ...be performed at global level from several different locations by an independent party.

## Policies & Procedures

A set of policies and procedures to be adopted by ALL DNS providers is required. These should cover (but not be limited to):

- SLAs
- Security Policies (staff security check requirements etc.)
- Regular Review of sites, policies and procedures
- Emergency Procedures
- Information Required to be maintained
- Procedures for emergency and after hours updates must be defined
- Must be accessible to ALL Operators

## Relationships

Early in the life of the Internet, facilities were shared and services provided on very informal basis, often referred to as 'Grace and Favour'. While this method may still work for some ccTLDs, or for some portion of a ccTLD's DNS Service, there is a growing trend toward formal, professional provision of services.

ccTLD managers must make sure that all relationships involved in provided DNS Services are documented and that the documentation includes the services being provided, the commitment the provider is making, and who is responsible for maintaining the relationship.

Relationships should be reviewed and confirmed at least once a year.

---

About the Author -

Chris Wright designed, configured and managed the construction of the current AusRegistry EPP Registry system on an open source Linux platform, which was the first Registry system in the world to feature "real time" dynamic DNS updates.

Chris has consulted and given many presentations to various Australian government departments and international forums on Registry principles, operation and maintenance of associated infrastructure

## Glossary:

- **"cache" "cached"** a temporary storage area where frequently accessed data can be stored for rapid access
- **AXFR** - A type of DNS transaction. It is one of the many mechanisms available for administrators to employ for replicating the databases containing the DNS data across a set of DNS servers
- **ccTLD** – country code Top Level Domain
- **DDOS** - Distributed Denial of Service attacks (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system
- **DNS Operators** - The employees within the DNS Provider that manage and maintain the “Name Service” and its associated equipment are the “DNS Operators”
- **DNS Provider** - An organisation that manages one or more “Name Service” is a “DNS provider”
- **DNS Service** is defined as the overall ability to locate the authoritative Name Servers for any third level (and in some cases fourth level) domain within the namespace. The collection of all Name Services that provide DNS resolution services for the namespace AND its associated sub-domains make up this overall DNS Service.
- **DNS Software** – software used to run DNS Services, such as ANS, BIND, CNS, djbdns, DNRD, dnsmasq, IPControl, IPM DNS, MaraDNS, MyDNS, NSD, Posadis, PowerDNS, Microsoft DNS, Simple DNS Plus, VitalQIP
- **DNSSEC** - Domain Name System Security Extensions
- **GLUED** - A glue record is an "A" record used to glue the DNS tree together
- **GMT** - Greenwich Mean Time
- **IETF** - Internet Engineering Task Force develops and promotes Internet standards

- **In-addr.arpa** - Used to convert 32-bit numeric IP addresses back into domain names (reverse DNS Lookup)
- **IP Address** - An IP address (Internet Protocol address) is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard
- **IPSEC** - IP security is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream
- **IPv4** - Internet Protocol version 4 is the fourth iteration of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed
- **IPv6** - The successor to IPv4 who's main improvement is the increase in the number of addresses available for networked devices
- **Name Servers** - An individual server that is responsible for providing DNS resolution services
- **Name Server Operators** - Manage and maintain the “Name Service” and its associated equipment are the “DNS Operators”
- **Name Server Site** - A site or more specifically the area within a site that is used to house Name Servers
- **Name Service** - A collection of Name Servers, that may or may not necessarily be located at the same Name Server Site, which respond to the same IPv4 and/or IPv6 address for the purpose of answering DNS queries.
- **NAPTR** - NAPTR stands for Naming Authority Pointer and is a newer type of DNS record that supports regular expression based rewriting
- **Network Intrusion Detection** - An intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic

- **Network Topology** - Network topology is the mapping of the elements (links, nodes, etc.) of a network, especially the physical (real) and logical (virtual) interconnections between nodes
- **NTP** - Network Time Protocol - The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency
- **RFCs** - Request for Comments (RFC) documents are a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies, The Internet Engineering Task Force (IETF) adopts some of the proposals published in RFCs as Internet standards.
- **RFC 1035** - Domain Implementation and Specification
- **RFC 2181** - Clarifications to the DNS Specification
- **Root-Server** - A root name server is a DNS server that answers requests for the root namespace domain, and redirects requests for a particular top-level domain (TLD) to that TLD's name servers.
- **SLAs** - Service Level Agreement (SLA) is that part of a service contract where the level of service is formally defined.
- **SOA** - Start of Authority. Each Zone contains one SOA Record, which holds the following properties for the Zone:
  - Name of Primary DNS
  - Mailbox of the Responsible Person
  - Serial Number
  - Refresh Retry Interval
  - Expire Interval
  - Minimum (default) TTL (Time To Live)
- **Source Routing** - Allows a sender of a packet to specify the route the packet takes through the network

- **SRV** - Service record is a category of data in the Internet Domain Name System specifying information on available services, defined in RFC 2782
- **STD40** - Host Access Protocol Specification
- **Stealth Primary** - A stealth primary is a name server that is inaccessible to the public
- **UDP** - User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite, using UDP, programs on networked computers can send short messages sometimes known as datagrams
- **WHOIS** - TCP-based query/response protocol which is widely used for querying a database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet
- **Zone File** - Contains information that defines mappings between domain names and IP addresses and can also contain reverse mappings which can resolve IP addresses into domain names