RIPE NetNews WG
Internet Draft
Document: draft-diaz-nhns-01.txt
Expires: February 2002

Daniel Diaz
RIPE NNWG
August 2002

NHNS - Netnews Hierarchy Names System

Status of this Memo

Comments should be sent to the author or the RIPE NetNews WG Mailing list: <netnews-wg@ripe.net>

Abstract

This document is focused on and describes one of the projects supported and carried out by the RIPE NetNews Working Group. NHNS is a system and service based on a DNS-like structure that has been discussed, developed and deployed under the umbrella of the RIPE NetNews Working Group. This is an update on the draft version published in October 2000.

Table of Contents

1. Introduction

This document defines the use of the known and regularly used DNS service as a database to store all the information related to Usenet (i.e. newsgroups, newsgroup descriptions, newsgroup moderators, grouplists, hierarchy maintainers, hierarchy descriptions, etc).This system is called Netnews Hierarchy Names System, hereafter referred to as "NHNS".

Familiarity with the DNS system [RFC1034, RFC1035] and the New DNS RR definitions [RFC1183] is assumed.

2. Origin and history of NHNS

NHNS emerged from the RIPE NetNews Working Group (NNWG) around May 1999. The NNWG agreed to create the 'groupsync project' just after suffering a 'fork-bomb' attack around May 1998(a form of DoS attack utilising high volume faked control messages) which caused many of the Usenet core servers to collapse

The initial goal of this project was providing the Usenet community with a consistent source of information to synchronize their servers in a secure and reliable way.

Several solutions were proposed but were never deployed, one based on a perl script collecting information from ftp and http resources and a second one based on the CVS software. The NHNS approach was proposed and presented in RIPE-34 (Vienna, May 1998) and received the support of the NetNews Working Group.

Nowadays netnews server software does much to reduce the effectiveness of such an attack (i.e. forkbomb attacks) as PGP processing of control messages is regularly serialized and it is therefore under control. However the benefits of a system offering access and coordination of Usenet administrative information, (i.e. newsgroup names, group lists, maintainers, maintainers PGP keys, newsgroup moderators) are still useful for administration, control and reference purposes.

3. Technical description

3.1 Introduction

NHNS is based on the well known and widely used DNS service and has benefited from community experience with DNS operational issues as well as existing DNS software implementations.

The hierarchical structure of Usenet group names and moderator information bears a significant resemblance to the structure of the DNS hierarchy. Based on this, NHNS maps group names to their descriptions using TXT resource records. And maps moderators' addresses using 'RP' resource records.

This approach was first deployed as a private DNS cloud. This cloud consisted of a fake top level domain called 'usenet.', under which all existing top level hierarchies (alt.*, comp.*,..., at.*, ch.*, de.*, es.*,...) were located, as shown in the figure below:

```
              .
             /
           usenet
        /\     \      \
       /  \     \      \
      /... \ ... \ ...  \
    ch     es    alt  comp
```

The structure described above, was supported by a faked root-server being the primary server for 'usenet.', and some secondary name servers for the same domain. Around a dozen collaborators participated in a small pilot, operating primary name servers for each of the hierarchies involved in addition to providing secondary name service for the 'usenet.' root zone.

This 'embryo' allowed the testing of the NHNS system in a semi-production environment as well as aiding the development of a small set of tools for use in retrieval and application of the data held in the NHNS system as explained in greater detail later in this document.

It should be kept in mind that a Usenet groupname represented in DNS is reversed, (i.e. similar to the representation of an IP address within the in-addr.arpa DNS tree) thus:

```
USENET groupname's order:  <group>.<category_n-1>.<...>.<tlh>

NHNS   groupname's order:  <tlh>.<category_1>.<...>.<group>
```

Following the test phase the fake DNS hierarchy rooted in 'usenet.' was relocated to an official DNS domain 'usenet.nhns.net.' giving the current DNS cloud shown below:

```
             .
            /
          net
         /
       nhns
      /
    usenet
   /  \     \        \
  /... \ ... \ ...... \
ch     es    alt    comp
```

The two experiences described above have proven the technical feasibility of the system and the value of the service.

3.2 Existing SW to support NHNS

The NHNS system has been designed to take advantage of the distributed database provided by the existing DNS system amd service. Another benefit of this approach being that it uses existing well proven software, no modification of any DNS sources are required to make NHNS work (i.e. bind, nsd, djdns, cachedns,... should work just fine).

3.3 Use of the TXT Resource Record

Format of the 'text' (TXT) resource record is specified in [RFC1183, section 3.3.14].

TXT records are used in NHNS to map groupnames to their descriptions as shown below:

```
news.es.    IN TXT   "Netnews group mapped in NHNS"
```

As shown above, the groupname is reversed when represented in DNS.

3.4 Use of the RP Resource Record

Format of the 'Responsible Person' (RP) resource record is specified in [RFC1183, section 2.2].

RP records are used in NHNS to map groupnames to their moderators' e-mail addresses as shown in the example below:

```
news.es.usenet.nhns.net. IN RP  es-news@rediris.es "Mod. for es.news"
```

The 'owner' field is the groupname in reverse order (i.e. news.es.usenet.nhns.net, representing es.news), the 'MBOX-DNAME' field is the group's moderator e-mail address in the Usenet's moderators file format (i.e. the one distributed by Tale). The 'TXT_DNAME' field will normally contain a comment.

3.5 Zone file considerations

In NHNS terminology a DNS zone-file is equivalent to a NetNews grouplist. A hierarchy name in NHNS is equivalent to a domain name (i.e. the es.* hierarchy grouplist is equivalent to the 'es.usenet.nhns.net.' DNS zone file data).

3.6 Client tools

An NHNS server may be queried using any of the available DNS client tools (i.e bind-tools like 'dig', 'named-xfer', 'nslookup', etc).

It should be noted in regard to these tools that while they can be used to query a nameserver for NHNS information, the information will be returned according to format of the TXT and RP records, which in terms of NHNS is reversed. This is shown in [3.3] and [3.4].

The circumstance described lead us to develop adapted tools to handle the DNS information to sort the groupnames and print them in the common 'Usenet' order, this set of tools is described below:

nhlookup:

Tool to issue single queries to a given DNS server for NHNS information.The description of the group and the moderators e-mail address in case it is a moderated group, will be obtained and sent to standard output.

nh-xfer:

Tool to obtain a grouplist of a supported hierarchy by performing a zone-transfer and translating the returned zone data into a common Usenet grouplist format.

nhtlh:

This tool can be used to obtain the list of authoritative nameservers for any of the existing TLHs.

newsync:

Used to synchronise the typical configuration files of a news server, being them, the 'active' and 'newsgroups' files.in an INN server, or It issues multiple zone-transfers to later process and file synchronization.

guins:

'guins' is a graphical user interfaced coded in Perl/Tk to provide an easy use of all the previous tools in a bundle.

All these tools and more information are available at http://www.nhns.net/

3.7 DNS updates

Thanks to the 'DNS UPDATE' feature, used by some of the existing NHNS-tools, a hierarchy maintainer is not enforced to set up and administrate a name server. This task could be delegated to any collaborator who would administrate the name server itself and would allow the official maintainer to update records (i.e maintain the grouplist remotely, ...), in the same way a maintainer sends a control message nowadays in order to create, delete, or modify a newsgroup.

4. Use of the NHNS service by news administrators

Right now, netnews server administrators may use the tools available with the different DNS implementations, like the existing and well-known bind-tools or the NHNS specific tools developed with the collaboration of the RIPE Netnews WG.

Administrators obtain many advantages from the NHNS service. Information such as the following can be obtained through a simple query:

- Verify correctness of grouplists, active, newsgroups and moderators files.

- Find the Responsible Person for a given TLH.

- Synchronise a news server by means of a zone-transfer.

- Look for a newsgroup description or moderator in a Usenet TLH.

5. Pending administrative issues

The current Usenet reliance on the regular distribution of administrative information (e.g. the moderators list posted by David Lawrence, the control.ctl file maintenance, the maintainer PGP keys, etc) is somewhat reminiscent of the hosts.txt philosophy which the DNS system was deployed to replace. The arguments put forward for this could easily be applied in the case of NHNS.

Since the beginning Usenet hierarchy maintainers have had trusted authority over their hierarchies and the related administrative data. Therefore the cooperation of maintainers would be required to successfully roll out the NHNS service.

As the NHNS service gathers necessary momentum, certain administrative issues will likely require to be solved by the respective organizations, like the possible creation of a new gTLD to support the system and the handing over of control of this to the appropriate party to control the delegation of the domains therein. Currently all the NHNS tree exists below the domain usenet.nhns.net. as a proof of concept, however this may not be appropriate in case this would become a public-wide service for the mentioned administrative reasons.

It should be born in mind however that this draft is concerned only with the technical feasibility of the service and that the above

paragraph is merely a suggestion of possible issues which may be presented in the course of further development.

6. Security considerations

The NHNS system and service makes use of the existing DNS service and structure, therefore all security issues related to DNS apply also to NHNS.

In practice, NHNS server administrators (i.e. nameserver administrators) must take care of the permissions to update resource records as well as the permissions to transfer zones. The following section will try to give some recommendations to a potential NHNS server administrator in order to secure the server.

6.1 Security recommendations

This section recaps the essential an administrator should know to secure a NHNS server.

When the first version of this draft was published, only IP filtering could be done with the existing BIND 8 versions, and this was not a warranty of security for DNS servers as IP-spoofing was enough to spoil our server's information, but, since BIND 8.2.3 there's the possibility to use nice security features like TSIG keys (or TSIG secrets), to encrypt DNS messages (i.e. secure the communication between two servers, an updater and a server, etc).

Normally an updater will only deal with one (or not many more) netnews hierarchy, so only one TSIG key is necessary. This makes TSIG a suitable feature regarding key management for the purpose of securing any DNS updates (i.e. updating a newsgroups list).

Nowadays, the Perl Module "Net::DNS: includes methods to support TSIG and other DNS-Sec features since version 0.21.

References

1 [RFC1183] New DNS RR Definitions. C.F. Everhart, L.A. Mamakos, R. Ullmann,P.V. Mockapetris. Oct-01-1990.

2 Elmar K. Vins, NHNS server configuration tutorial http://www.nhns.net/nhns/DOC/nhnstutorial-1.0.txt September 1999.

3 Daniel Diaz, newsync command tutorial http://www.nhns.net/nhns/DOC/newsync.txt. October 1999.

4 [RFC2136] P. Vixie (Ed.), S. Thomson, Y. Rekhter, J. Bound Dynamic Updates in the Domain Name System," RFC 2136, ISC & Bellcore & Cisco & DEC, April 1997.

5 [RFC2137] Secure Domain Name System Dynamic Update. D. Eastlake. April 1997.

6 [SSU]   B. Wellington, "Simple Secure Domain Name System (DNS) Dynamic Update, " draft-ietf-dnsext-simple-secure-update-01.txt, Nominum, May 2000.

Acknowledgments

- Juan Garcia (SATEC, S.A): Who is half the inventor of this evil thing.
- Dave Knight (RIPE NCC): for a wonderful help adapting this text into English)
- Dave Wilson (HeaNet): for donating the NHNS.NET. domain.
- Jose M. Femenia (& all the UV): for hosting nhns.uv.es. and more.
- Olaf Kolkman (RIPE NCC): for helping to solve the Net::DNS bugs.
- Felix Kugler (SWITCH), Gerhard Winkler (ACONET)for their support.
- All OPS at RIPE NCC for their support.

Author's Addresses

Daniel Diaz Luengo
RIPE NNWG
Singel 258, 1016AB Amsterdam, The Netherlands
Phone: +31 20 535 4444
Email: Daniel.Diaz@ripe.net, Daniel.Diaz@nhns.net