Domain Name Working Group
Request for Comments: DRAFT
Expires: October 2006
Document: draft-msullivan-dnsop-generic-naming-schemes-00.txt
April 2006

Matthew Sullivan
Spam and Open Relay Blocking System
Luis Munoz
CANTV

Suggested Generic DNS Naming Schemes for Large Networks and Unassigned hosts.

Status of this Memo

Abstract

This memo describes basic DNS configurations and details suggestions for a common naming scheme for records that are automatically generated and therefore likely generic in nature. This memo will re-iterate issues highlighted in a number of other RFCs such as RFC 1912.

Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

TABLE OF CONTENTS

MEMO STATUS 1

ABSTRACT 1

NOTATION 2

TABLE OF CONTENTS 2

1. INTRODUCTION 2

2. BACKGROUND 3

3. GENERIC RECORDS 4

4. Allocation Type Assignment Indicators 5
   4.1. Static address ranges 5
   4.2. Dynamic Address Ranges 6
   4.3. Unassigned Address Ranges 7

5. Transport Type Assignment Indicators 7
   5.1. DSL link transport indicators 8
   5.2. Dial-Up transport indicators 8
   5.3. Cable modem terminated link indicators 9
   5.4. Mobile device (GPRS, WiFi etc) 9
   5.5. Address ranges assigned to multi purpose links 10
   5.6. Address ranges assigned to leased lines and ATM links 11

6. Customer Type Assignment Indicators 12
   6.1. Address ranges assigned to business customers 12
   6.2. Address ranges assigned to residential customers 12
   6.3. Address ranges assigned to co-location customers 13
   6.4. Address ranges assigned to shared server customers 13

7. Server/Machine Type Assignment Indicators 14
   7.1. Address ranges assigned to mail servers 14

7.1.1. Assignments for incoming mail servers 14
7.1.2. Assignments for incoming and outgoing mail servers ... 15
7.1.3. Assignments for outgoing mail servers 15
7.2. Address ranges assigned for web servers 16
7.3. Address ranges assigned for DNS servers 16

7.4. Address ranges assigned for core infrastructure 17
7.5. Address ranges assigned for multi-purpose hosts 17

8. Language Issues in Naming Schemes 18

9. Miscellaneous Items with Respect to Naming Schemes 18

10. DNS Requirements 19

11. Security Considerations 19

12. Acknowledgements 19

13. References 19

Copyright and Disclaimer 20

Author's Address 21

1. Introduction

All Internet connected hosts should have a host name which will identify its IP address as well as an entry in the IN-ADDR.ARPA. domain indicating its host name.

For large IP address lists it can be impractical to give each host and individual host name and record that host name for both A DNS RRs and PTR DNS RRs. To make the task of providing individual records for net blocks simpler, various facilities are available to generate zone files. Large zone files can be very impractical to manipulate so some DNS servers allow for a keyword to format and generate mass zone data internally within the running server.

Unfortunately, the use of these generated records has resulted in a significant difficulty for remote networks to identify the perpetrators of varying forms of network abuse.

This memo will not provide syntactical detail of the commands or scripts used. It will however, suggest a common naming scheme for use in automatically generated zones where zones cannot be crafted with the actual host names of the machines.

2. Background

The need for a common format is becoming more and more apparent in the fight against abuse. The abuse across the Internet began in the early days of the Network and took many forms, from hacking and

cracking, to abusing open SMTP relays and proxy servers for the propagation of spam.

Those who have taken it upon themselves to attempt to stop this abuse of resources, and those who are tasked with investigating the source of the abuse, seem to come up against a number of issues relating to the identification of the source of the abuse.

The identification of the source of abuse is a problem for many reasons, first the IP address to host mapping often will give no indication of the appropriate services the host does provide. It gives no clue as to whether the abuse attempt on one IP address in a network followed by a second is the same host attempting the same abuse or whether there are multiple hosts involved. The host mapping will often either not exist or, refer to a non-existent host name with little or no indication of the person responsible or organisation for abuse issues arising from the host.

Clear identification and records for a host and network would resolve most of issues relating to the identification of abusing or abused hosts. Identification that includes reasonable information as to the purpose or configuration of the host will also allow other networks to configure access, thereby limiting abuse, using these identification records.

3. Generic Records

Generic records are the most basic form of host names and are used in large networks where the administrators of those networks have classes of hosts all similar in type. The administrators of the records often will not have access to the configuration of the hosts as they will typically be 'customer' machines.

Generic records are typically seen as records configured like the following example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.example.com.
1       IN  PTR    1.0.0.10.example.com.
.
.
254     IN  PTR    254.0.0.10.example.com.
255     IN  PTR    255.0.0.10.example.com.
```

Typically these hosts offer no information about their purpose, nor whether they are actually allocated. For that reason where access is restricted in any way it is expected that hosts in this networks will be granted no special privilege, and in many cases may be denied

access.

4. Allocation Type Assignment Indicators

The following sub-sections gives suggested naming schemes for generic static, dynamic and unassigned address blocks. The naming schemes are not mandatory, but are strongly recommended for the sake of consistency.

Regardless of the nature of the address block, the names configured in the DNS IN-ADDR.ARPA zone SHOULD contain the domain name of the organization responsible for the operation of the hosts at its rightmost position.

4.1. Static Address Ranges

In static host allocations, the IP addresses have been assigned to an individual host in a persistent matter. This can be by manually configuring the host's network interface(s) with a non-volatile configuration, or by the use of host configuration protocols such as DHCP in a manner that guarentees that the same host will always receive the sane IP address. It should be noted that to be considered static the interface MUST be configured to the same address every time it is connected to the Internet.

DNS RRs for statically configured hosts SHOULD echo the fully qualified real name(s) of the host. Where this is not possible and subnet delegation, as described in RFC 2317 is not possible generic records MUST be used. To comply with RFC 1912 all PTR DNS RRs MUST have corresponding A RRs. The format of the PTR records SHOULD indicate that the hosts are statically allocated their addresses. The suggested format for the records is as follows:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.static.example.com.
1       IN  PTR    1.0.0.10.static.example.com.
.
.
254     IN  PTR    254.0.0.10.static.example.com.
255     IN  PTR    255.0.0.10.static.example.com.
```

Where the DNS resolution provider is concerned with respect to resources, and/or the provider is using additional information convention, the word 'static' MAY be abbreviated to 'sta', for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.sta.example.com.
```



```
1       IN  PTR    1.0.0.10.sta.example.com.
.
.
254     IN  PTR    254.0.0.10.sta.example.com.
255     IN  PTR    255.0.0.10.sta.example.com.
```

The static identifier MUST be presented as the identifier nearest the sub domain or domain name where used.

The static identifier MUST only be used when the organization responsible for the operation IN-ADDR.ARPA. zone able to accurately map an IP address to the host that this address was assigned to at any given date and time.

4.2. Dynamic Address Ranges

In dynamic host allocations, the hosts addresses are configured at runtime and may change at any predetermined interval. This type of allocation is typically acheived by configuring the host's network interface(s) through protocols like DHCP. PPP up links whether dial up, PPP over Ethernet or PPP over ATM typically will not know either one of the endpoints and MUST be considered as dynamically allocated.

DNS RRs for dynamically configured hosts SHOULD NOT echo the fully qualified real name(s) of the host as the information is likely to change without warning. Generic records MUST be used for dynamically allocated networks. To comply with RFC 1912 all PTR DNS RRs MUST have corresponding A RRs. The format of the PTR records SHOULD indicate that the hosts are dynamically allocated their addresses. The suggested format for the records is as follows:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.dynamic.example.com.
1       IN  PTR    1.0.0.10.dynamic.example.com.
.
.
254     IN  PTR    254.0.0.10.dynamic.example.com.
255     IN  PTR    255.0.0.10.dynamic.example.com.
```

Where the DNS resolution provider is concerned with respect to resources, and/or the provider is using additional information convention, the word 'dynamic' MAY be abbreviated to 'dyn', for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.dyn.example.com.
1       IN  PTR    1.0.0.10.dyn.example.com.
.
```



```
.
254     IN  PTR    254.0.0.10.dyn.example.com.
255     IN  PTR    255.0.0.10.dyn.example.com.
```

The dynamic identifier MUST be presented as the identifier nearest the sub domain or domain name where used.

4.3. Unassigned Address Ranges

Unassigned address ranges are where the address range is allocated to an organisation and the addresses have no hosts using them, nor are any hosts expected to use them in the immediate future.

Note: Ranges configured for hosts but as yet with no hosts connected MUST NOT be considered 'Unassigned'.

Unassigned ranges MUST be configured for DNS by EITHER having no PTR records for the range OR by using the keyword 'unassigned' in host names specified in the IN-ADDR.ARPA. domain. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.unassigned.example.com.
1       IN  PTR    1.0.0.10.unassigned.example.com.
.
.
254     IN  PTR    254.0.0.10.unassigned.example.com.
255     IN  PTR    255.0.0.10.unassigned.example.com.
```

Unlike other types of PTR record it is acceptable though not advised to use the same host name in every PTR record, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    unassigned.example.com.
1       IN  PTR    unassigned.example.com.
.
.
254     IN  PTR    unassigned.example.com.
255     IN  PTR    unassigned.example.com.
```

5. Transport Type Assignment Indicators

The following sub-sections suggest and recommend naming conventions for the more common type of transport type indicators. These are not mandatory indicators, however it is recommended that if transport type indicators are to be used the following indicators SHOULD be used for consistency.

Allocations type assignment indicators [Section 4] MUST be configured whenever Transport type indicators are used.

5.1. DSL Transport Indicators

DSL transport indicators for address ranges are where the address range is solely used for DSL end points regardless of static assignment or customer type. DSL transport is identified by the use of the 'dsl' indicator in host names specified in the IN-ADDR.ARPA. domain. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.dsl.dyn.example.com.
1       IN  PTR    1.0.0.10.dsl.dyn.example.com.
.
.
254     IN  PTR    254.0.0.10.dsl.sta.example.com.
255     IN  PTR    255.0.0.10.dsl.sta.example.com.
```

Where more specific DSL Transport type indicators are required the 'dsl' identifier SHOULD be prefixed with a type abbreviation. Valid type abbreviations are as follows:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.adsl.dyn.example.com.
                             ; ADSL and ADSL2
1       IN  PTR    0.0.0.10.sdsl.dyn.example.com.
                             ; Symmetric DSL
.
.
254     IN  PTR    0.0.0.10.shdsl.sta.example.com.
                             ; Symmetric High speed DSL
255     IN  PTR    0.0.0.10.a2dsl.sta.example.com.
                             ; ADSL2
```

5.2. Dial-Up Transport Indicators

Dial-Up transport indicators for address ranges are applicable when the range is solely used for end points that have to dial access numbers via PSTN.

Dial-up transport is identified by the use of the 'dial' indicator in host names specified in the IN-ADDR.ARPA. domain. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.dial.dyn.example.com.
1       IN  PTR    1.0.0.10.dial.dyn.example.com.
```

```
        .
        .
        254      IN   PTR    254.0.0.10.dial.sta.example.com.
        255      IN   PTR    255.0.0.10.dial.sta.example.com.
```

Where most specific Dial-Up Transport type indicators are required the 'dial' identifier SHOULD be replaced with a more specific indicator such as:

```
        $ORIGIN 0.0.10.IN-ADDR.ARPA.
        0        IN   PTR    0.0.0.10.isdn.dyn.example.com.
                                          ; ISDN connections
        1        IN   PTR    1.0.0.10.dov.dyn.example.com.
                                          ; Digital Over Voice ISDN
        .
        .
        254      IN   PTR    254.0.0.10.modem.sta.example.com.
                                          ; Standard Analog Modem
        255      IN   PTR    255.0.0.10.modem.dyn.example.com.
                                          ; Standard Analog Modem
```

5.3. Cable Modem Transport Indicators

Cable modem transport indicators for address ranges are appropriate when the range is solely used for end points that are terminated at cable modems.

Cable transport type is identified by the use of the 'cable' indicator in host names specified in the IN-ADDR.ARPA. domain. For example:

```
        $ORIGIN 0.0.10.IN-ADDR.ARPA.
        0        IN   PTR    0.0.0.10.cable.dyn.example.com.
        1        IN   PTR    1.0.0.10.cable.dyn.example.com.
        .
        .
        254      IN   PTR    254.0.0.10.cable.sta.example.com.
        255      IN   PTR    255.0.0.10.cable.sta.example.com.
```

5.4. Mobile Device Indicators

Mobile device indicators are provided for address ranges where the range is used for transport types associated with mobile devices, for example, laptop computers with wireless network interfaces, mobile phones, etc. Where the provider does not wish to distinguish the type of connected device, the provider SHOULD use the 'wireless'

token, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0        IN  PTR    0.0.0.10.wireless.dyn.example.com.
1        IN  PTR    1.0.0.10.wireless.dyn.example.com.
.
.
254      IN  PTR    254.0.0.10.wireless.sta.example.com.
255      IN  PTR    255.0.0.10.wireless.sta.example.com.
```

For networks where the provider wishes to identify the connecting host more accurately, the following tokens SHOULD be used:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0        IN  PTR    0.0.wifi.dyn.example.com. ; WiFi Devices
1        IN  PTR    0.1.gprs.dyn.example.com. ; GPRS devices
.
.
254      IN  PTR    0.254.cdma.dyn.example.com. ; CDMA devices
255      IN  PTR    0.255.bt.dyn.example.com.   ; Bluetooth
```

This list is expandable and care should be exercised when choosing tokens that are not explicitly specified.

5.5. Multi-Purpose Transport Indicators

Multi-purpose transport indicators are provided for address ranges that are used for multiple transport types. For example, a service which provides ADSL connectivity with backup dial up would be better identified as a multi type, or by the primary (in this case ADSL) indicator.

Multiple transport type addresses are identified by the use of the 'multi' indicator in host names specified in the IN-ADDR.ARPA. domain. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0        IN  PTR    0.0.0.10.multi.dyn.example.com.
1        IN  PTR    1.0.0.10.multi.dyn.example.com.
```

```
         .
         .
         254      IN   PTR    254.0.0.10.multi.sta.example.com.
         255      IN   PTR    255.0.0.10.multi.sta.example.com.
```


5.6. Dedicated links

ATM and dedicated transport indicators for address ranges are where the range is solely used for networks that are connected via ATM, leased line or other types of dedicated connection.

Generally ATM and leased line links SHOULD have host names connected, however where generic naming is required the following tokens SHOULD be used:

```
         $ORIGIN 0.0.10.IN-ADDR.ARPA.
         0        IN   PTR    0.0.0.10.atm.dyn.example.com. ; ATM
         1        IN   PTR    1.0.0.10.eth.dyn.example.com. ; Ethernet
         2        IN   PTR    2.0.0.10.ll.dyn.example.com.  ; Leased Line
         3        IN   PTR    3.0.0.10.mwv.sta.example.com. ; Microwave
         .
         .
         50       IN   PTR    50.0.0.10.oc3.sta.example.com. ; OC3
         51       IN   PTR    51.0.0.10.e3.sta.example.com.  ; E3
         52       IN   PTR    52.0.0.10.t1.sta.example.com.  ; T1 (etc.)
         .
         .
         253      IN   PTR    253.0.0.10.giga.sta.example.com.  ; Gigabit
         254      IN   PTR    254.0.0.10.fiber.sta.example.com. ; Fiber
         255      IN   PTR    255.0.0.10.laser.sta.example.com. ; LASER
```

As the types of transport described in this section are mostly fixed, the use of the token 'dedicated' MAY be used where specific typing is not desired.

The 'dedicated' token MUST NOT be used for networks where the assignments are dynamic. The 'dedicated' token can be using in place of the 'static' token described in 4.1.

The 'dedicated' token can be shortened to 'ded' for resource economy. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0       IN  PTR    0.0.0.10.dedicated.example.com.
1       IN  PTR    1.0.0.10.dedicated.example.com.
.
.
254     IN  PTR    254.0.0.10.ded.example.com.
255     IN  PTR    255.0.0.10.ded.example.com.
```


6. Consumer Type Assignment Indicators

The following sub-sections suggest and recommend naming conventions for the more common types of consumer transport type indicators. These are not mandatory indicators, however it is recommended that if consumer type indicators are to be used the following indicators SHOULD be used for consistency.

Allocations type assignment indicators [Section 4] MUST be configured whenever consumer type indicators are used, and the addresses are assigned dynamically.

6.1. Business Customers Addresses

Business consumer indicators for address ranges are where the range is solely used for networks that are connected to business customers.

Generally business consumers SHOULD have host names of machines connected, however where generic naming is required the following tokens SHOULD be used:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0        IN  PTR    0.0.0.10.biz.dyn.example.com.
1        IN  PTR    1.0.0.10.biz.dyn.example.com.
.
```

```
      .
      254       IN   PTR    254.0.0.10.biz.sta.example.com.
      255       IN   PTR    255.0.0.10.biz.sta.example.com.
```

6.2. Residential Customer Addresses

Residential consumer indicators for address ranges are where the range is solely used for networks that are connected to residential customers, including residential networks at educational institutions.

Generally, residential consumers will not have host names of machines connected, however the IN-ADDR.ARPA. zone MUST have records identifying the connectivity provider. Generic naming SHOULD use the 'client' or 'res' token. For educational institutes it is common to use the token 'resnet', this token is also acceptable.

An allocation type assignment tokens [Section 4] MUST be used with the residential customer type indicator, for example:

```
      $ORIGIN 0.0.10.IN-ADDR.ARPA.
      0         IN   PTR    0.0.0.10.res.dyn.example.com.
```



```
      1         IN   PTR    1.0.0.10.client.dyn.example.com.
      .
      .
      254       IN   PTR    254.0.0.10.client.sta.example.com.
      255       IN   PTR    255.0.0.10.res.sta.example.com.
```

6.3. Co-Location Customers and Address Ranges

Co-location customers are those providing their own dedicated hardware which is located within a providers network. Co-location customers SHOULD have their own records, however where the provider decides not to provide specific host name support within the IN-ADDR.ARPA. domain the 'colo' assignment token MUST be used.

An allocations type assignment token [Section 4] is not expected to be used for co-location servers when assigned static addresses. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    0.0.0.10.colo.example.com.
1         IN   PTR    1.0.0.10.colo.example.com.
.
.
254       IN   PTR    254.0.0.10.colo.example.com.
255       IN   PTR    255.0.0.10.colo.example.com.
```

In the unusual configuration that co-location ranges are assigned dynamically the 'dyn' allocation type token MUST be used. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    0.0.0.10.colo.dyn.example.com.
1         IN   PTR    1.0.0.10.colo.dyn.example.com.
.
.
254       IN   PTR    254.0.0.10.colo.dyn.example.com.
255       IN   PTR    255.0.0.10.colo.dyn.example.com.
```

6.4. Shared Server Addresses

Shared server addresses are used for a providers' address range where the servers house multiple consumers and where a single address may have a number of customers assigned. Shared server addresses SHOULD have the host name of the machine in the IN-ADDR.ARPA. domain. Where the service provider chooses not to use the host name or customer supplied host name of the machine in the IN-ADDR.ARPA. domain,

generic records MUST be used. A generic record for a shared server SHOULD include the 'shared' token, but MAY replace it with a token identifying the service provided [See Section 7], for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    0.0.0.10.shared.example.com.
1         IN   PTR    1.0.0.10.shared.example.com.
.
.
254       IN   PTR    254.0.0.10.shared.example.com.
255       IN   PTR    255.0.0.10.shared.example.com.
```

As with co-location ranges, is it unusual for shared server addresses to be assigned dynamically, so the 'dyn' allocation type token MUST be used where the addresses are not assigned statically.

7. Server Type Assignment Indicators

Server type assignment indicators are used where servers are to be identified by remote servers and services for a specific type of traffic. Use of these indicators should be used carefully as DNS provides the WKS RR type, the assignment indicators should still be used in conjunction with the WKS RR type as there is no current method to map IP addresses to services.

Server type indicators should not normally be used in generic records as generic records are used where it is impractical to set individual customer host names. Server type indicators for generic records are provided for large organisations where there is a large cluster of machines with the same purpose.

Unlike with other generic indicators the server type indicator MUST prefix the host name in the DNS RR.

7.1. Mail Server Indicators

Often in large networks, the purpose of mail servers is not to send and receive mail, but send mail or receive mail. For that reason the identifiers have been split into three main tokens, one for general mail servers, one for incoming only mail servers and one for outgoing only mail servers.

7.1.1. Incoming Mail servers

Incoming mail servers MUST HAVE both a DNS RR of type A and a DNS RR of type PTR, both DNS RRs MUST be complementary. The DNS RRs SHOULD match the host name of the server so that the host name presented in

the mail server's response to the HELO or EHLO commands matches the host name in the A and PTR records. In large networks it is often desirable to use a generic name to identify the host without tying public records to specific hardware. This is particularly important when using load balancers and similar hardware. Suggested tokens for use as the incoming MX host names is the token 'mx' which would normally prefix a number identifying the pool member. The 'mx' token SHOULD be the first characters of the host name, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    mx0.example.com.
1         IN   PTR    mx1.example.com.
.
.
254       IN   PTR    mx254.example.com.
255       IN   PTR    mx255.example.com.
```

7.1.2. Incoming and Outgoing Mail servers

Incoming and outgoing mail servers MUST HAVE both a DNS RR of type A and a DNS RR of type PTR, both DNS RRs MUST be complementary. The DNS RRs SHOULD match the host name of the server so that the host name presented by the mail server's response to the HELO or EHLO commands matches the host name in the A and PTR records.

Normally servers will not have generic host names when they are both incoming and outgoing servers, however in the event that this configuration is required, the 'mail' token should be used to prefix host name in the PTR record. For example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    mail0.example.com.
1         IN   PTR    mail1.example.com.
.
.
254       IN   PTR    mail254.example.com.
255       IN   PTR    mail255.example.com.
```

7.1.3. Outgoing Mail servers

Outgoing mail servers MUST HAVE both a DNS RR of type A and a DNS RR of type PTR, both DNS RRs MUST be complementary. The DNS RRs SHOULD match the host name of the server so that the host name presented in the mail server's response to the HELO or EHLO commands matches the host name in the A and PTR records. It is often desirable to use a generic name to identify the host without tying public records to specific hardware. Suggested tokens for use as the outgoing mail servers is the token 'mail' or 'smtp' which would normally prefix a number identifying the pool member. The 'mail' or 'smtp' token SHOULD be the first characters of the host name, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    mail0.example.com.
1         IN   PTR    mail1.example.com.
.
.
254       IN   PTR    smtp254.example.com.
255       IN   PTR    smtp255.example.com.
```

7.2. Web Servers

Web servers SHOULD be identifiable with DNS RRs of type PTR. For that reason when deploying clusters of web servers for the same sites, they SHOULD be identified with the prefix token of 'www' whenever generic host names are used, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    www0.example.com.
1         IN   PTR    www1.example.com.
.
.
254       IN   PTR    www254.example.com.
255       IN   PTR    www255.example.com.
```

7.3. DNS Servers

DNS server SHOULD be identifiable with DNS RRs of type PTR. It is relatively unusual for large clusters of DNS servers to be deployed, further it is not advised to deploy clusters of DNS servers on the same IP ranges except in special configurations. DNS servers are usually identified in NS and A RRs with the 'ns' token prefixed to a numeric value, therefore the same token SHOULD be used for the DNS RRs of type PTR, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    ns0.example.com.
1         IN   PTR    ns1.example.com.
.
.
254       IN   PTR    ns254.example.com.
255       IN   PTR    ns255.example.com.
```

7.4. Core Infrastructure

Core infrastructure SHOULD NOT be named in a generic fashion, each name SHOULD be used as a unique identifier for the piece of equipment. The non generic names of the devices does not have to indicate any meaningful information to third parties. Core infrastructure SHOULD use the token 'core' to identify it as a core device, for example:

```
  $ORIGIN 0.0.10.IN-ADDR.ARPA.
  0         IN   PTR
fastethernet3-1.dkn4-core.canberra.example.com.
  1         IN   PTR    gigabitethernet3-0.dkn-
core1.canberra.example.com.
  .
  .
  54        IN   PTR    pos4-1.ken-core4.sydney.example.com.
  55        IN   PTR
10gigabitethernet2-2.core02.sydney.example.com.
  .
  .
  254       IN   PTR    i-2-0.dal-core01.example.com.
  255       IN   PTR    i-10-0.chi-core01.example.com.
```

7.5. Multi-Purpose Hosts

Multi-purpose servers SHOULD be identifiable with DNS RRs of type PTR. Multi-purpose servers are not servers defined in 6.4. of this document, but are servers where multiple public services are deployed. Where the operator does not wish to identify a local service, for any reason, and chooses to use a generic name for the DNS RRs the server SHOULD be identified by the token 'srv'. For example:

```
  $ORIGIN 0.0.10.IN-ADDR.ARPA.
  0         IN   PTR    10.0.0.0.srv.example.com.
  1         IN   PTR    10.0.0.1.srv.example.com.
  .
  .
```

```
        254       IN   PTR    10.0.0.254.srv.example.com.
        255       IN   PTR    10.0.0.255.srv.example.com.
```

If the 'srv' token is used for dynamically allocated hosts the 'srv' token MUST suffix a 'dyn' token as described in Section 4.2 of this document.

8. Language Issues in Naming Schemes

The author of this document notes, and acknowledges, that there are some truly beautiful languages around the world, however the naming scheme proposes English tokens as the majority population of the Internet speaks English when communicating with persons of another country, as English is almost a common language.

9. Miscellaneous Items with Respect to Naming Schemes

The author also notes that the naming scheme proposed is not comprehensive with respect to devices, and suggests that sensible choices should be made when introducing new tokens to your networks. Particular care should be taken with respect to how others may wish to automate access based upon the device type and use, this is particularly important when considering connections to other organisation's mail servers and other public services.

Care and consideration should be taken before assigning vendor names to devices, for example when choosing names for devices and questions like; could the device be replaced in the future by another vendors product?

When using IP addresses in host names, their numbers SHOULD be separated by '.'s (dots) rather than any meta character such as a '-' (dash) and expressed in decimal. Host names SHOULD NOT use the '_' (underscore) character, host names for hosts with any form of SMTP mail service MUST NOT use the '_' (underscore) character. It is preferable to use the IP address in reverse format in the same way the the IN-ADDR.ARPA. domain is defined.

Data repetition MUST be avoided, as MUST redundant (and incorrect) references to the fact that the DNS RR is a PTR, reverse DNS, part of the IN-ADDR.ARPA zone. For example, do not use the tokens 'ptr', 'rev', 'in-addr', 'in-addr.arpa' just to indicate the record is within the IN-ADDR.ARPA. domain. Examples of data repetitions would be: 10gigabitethernet2-2.syd-core02.sydney.example.com ('syd' makes 'sydney' redundant).

Where Location specific data and tokens describe in Sections 4 and 6 are used the location data MUST prefix the tokens from Sections 4 and/or 6, for example:

```
$ORIGIN 0.0.10.IN-ADDR.ARPA.
0         IN   PTR    10.0.0.0.syd.dyn.example.com.
1         IN   PTR    10.0.0.1.syd.res.dyn.example.com.
.
.
```



```
254       IN   PTR    10.0.0.254.ny.bus.sta.example.com.
255       IN   PTR    10.0.0.255.paris.res.sta.example.com.
```

10. DNS Requirements

The DNS service and naming schemes MUST conform to other current RFCs and BCPs.

All DNS RRs of type PTR MUST have a corresponding DNS RR of type A.

Generic naming schemes across multiple networks SHOULD NOT be used unless the network is dynamically allocated. Generic records SHOULD be used where networks are dynamically allocated.

11. Security Considerations

This RFC does not define any new services or protocols. The authors of this memo acknowledge that it includes recomendations for the adoption of a publicly accesible naming scheme that provides information about network allocations and for services provided at different network hosts.

This information is at least partialy available in many ways such as existing naming schemes, the Internet's routing table and WHOIS (RFC 3912) information. Additionally, current network threat models make the scanning of large network allocations a non-issue for an attacker. Further, mail and DNS servers are easily identified by other methods.

12. Acknowledgements

Steven Champeon

Luis Munoz

13. References

[RFC 1033] Lottor, M, "Domain Administrators Operations Guide", RFC 1033, USC/Information Sciences Institute, November 1987.

[RFC 1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

[RFC 1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.

[RFC 1123] Braden, R., "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, IETF, October 1989.

[RFC 1178] Libes, D., "Choosing a Name for Your Computer", FYI 5, RFC 1178, Integrated Systems Group/NIST, August 1990.

[RFC 1183] Ullman, R., Mockapetris, P., Mamakos, L, and C. Everhart, "New DNS RR Definitions", RFC 1183, October 1990.

[RFC 1535] Gavron, E., "A Security Problem and Proposed Correction With Widely Deployed DNS Software", RFC 1535, ACES Research Inc., October 1993.

[RFC 1536] Kumar, A., Postel, J., Neuman, C., Danzig, P., and S. Miller, "Common DNS Implementation Errors and Suggested Fixes", RFC 1536, USC/Information Sciences Institute, USC, October 1993.

[RFC 1537] Beertema, P., "Common DNS Data File Configuration Errors", RFC 1537, CWI, October 1993.

[RFC 1912] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, The Pennsylvania State University, February 1996

[RFC 2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, AT&T Laboratories, April 2001.

[RFC 3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, VeriSign, Inc., September 2004.

[RFC 4084] Klensin, J., "Terminology for Describing Internet Connectivity", RFC 4084,, May 2005.

[BOG] Vixie, P, et. al., "Name Server Operations Guide for BIND", Vixie Enterprises, July 1994.

Copyright and Disclaimer

Author's Address:

Matthew Sullivan
Spam and Open Relay Blocking System
Po Box 5150

Bruce, ACT 2617
Australia

Email: matthew@sorbs.net

Luis Munoz
Av. Libertador
Centro Nacional de Telecomunicaciones
Edif. NEA, Piso 14
Caracas - Venezuela, 1010

Email: lem@sorbs.net