# Domain Name System References

Red Hat Linux 7 and 6.2 customers who subscribe to the Red Hat Network got fixes for the widely -reported security hole in the Berkeley Internet Name Domain software key to Internet reliability.

* RFC 1034 – Domain Names – Concepts and Facilities
* RFC 1035 – Domain Names – Implementation and Specification
* BOOK: Paul Albitz and Cricket Liu, DNS and BIND, O'Reilly & Associates.
* Web Site: “DNS Resources Directory”, <http://www.dns.net/dnsrd>
* man pages (named, resolv.conf)

##### Notes:

DNS server (name server) maps a name to an ip address. The client that requests the name/ip address is called a “name resolver”, (recursive resolution, iterative resolution).

We have said that queries to name refer to local names. In the two-step name resolution process, resolution begins with the local name server. If the local server cannot resolve a name, the query must be sent to another in the domain.

Most name resolution refers to local names, those found the same subdivision of the namespace as the machine from which the request originates.

The namespace is partitioned at the top level (parent), and authority for names in subdivision is passed to a designated agent. For example we might choose a partition based on the site name.

Syntactically, subdividing the namespace introduces another partition of the name. For example adding a “Group” subdivision to names already partitioned by site procedures, example: (local.group.site).

Tracing a path through the hierarchy to contact the local authority would be inefficient. Second, if each name resolution always started by contacting the topmost level of the hierarchy, the machine at that point would become overloaded.

Internet name servers use “name caching” to optimize search costs. Keeping a copy of the local servers database in each host has several advantages. Obviously, it makes name resolution on local hosts extremely fast because it means the host can resolve name without any network activity.

DNS servers also resolve MX records which is electronic mail exchangers. It allows a site to specify multiple machines that are each capable of accepting mail.

The mail exchangers steps through the set from highest preference to lowest (lower numbers mean higher performance).

It tries to contact the host and deliver mail. If the host is unavailable, the mailer will continue trying other hosts on the list. (mail gateways, mail bridges, mail relays or intermediate mail).

Domain names; (com, edu, gov, mil, net, org, arpa, int):

A subtree of names managed by a given name servers forms a “zone of authority”.

Fundamentals

##### Resolver

* Send Name Queries to Name Server on behalf of local programs
* Parse Responses from Name Server and give results to local programs
* Config. File (UNIX: /etc/resolv.conf, NT: Control Panel – Network – Protocols – TCP/IP Protocol – Properties - DNS)

##### Name Server

* Receive DNS Queries and Provide Response Information
* Config. File (UNIX: /etc/named.boot, NT: \Winnt\System32\Dns\Boot)

resolv.conf

* Rubicon /etc/resolv.conf
* domain net.sec.com
* search net.sec.com tis.com
* nameserver 10.0.1.144

named.boot

* Reduced Rubicon /etc/named.boot

directory /var/named

cache . root.cache

primary 0.0.127.in-addr.arpa named.127.0.0

secondary hq.sec.com 10.33.1.2 zone.hq.tis.com

secondary 33.10.in-addr.arpa 10.33.1.2 zone.10.33

primary net.sec.com named.net.sec.com

primary trusted.com named.sec.com

primary 155.55.76.in-addr.arpa named.154.54.75

primary 0.10.in-addr.arpa named.10.0

forwarders 10.0.1.128 10.0.1.128

slave

**Zone File**

* Reduced Rubicon /var/named/named.net.sec.com

@ IN SOA net.sec.com. postmaster.sec.com. (

1998082000 ; serial

3600 ;refresh

3600 ; retry

604800 ; expire - 1 weeks

7200 ) ;TTL

IN NS net.sec.com.

MX 10 net.sec.com.

IN A 10.0.1.144

localhost IN A 127.0.0.1

;

; LAB NT Test Computers

;

nttest01 IN A 204.254.155.98

nttest02 IN A 204.254.155.99

nttest05 IN A 204.254.155.100

Reverse Zone File

@ IN SOA net.sec.com. root.net.sec.com. (

1998071600 ; Serial

3600 ; Refresh

3600 ; Retry

604800 ; Expire

7200 ) ; Minimum

IN NS net.sec.com.

98 IN PTR nttest01.net.sec.com.

99 IN PTR nttest02.net.sec.com.

100 IN PTR nttest05.net.sec.com.

Zone File Hints

* Manually Change Serial Number or Else
* Dot at End of Domain Name Spec.s
* Blanks in Left-Most Field
* Comments are “;” NOT “#”

#### Firewall Considerations

* Outside Systems Should Not See Inside Names and Addresses
* No “DNS Proxy” – Inside Systems Cannot Use Outside Name Servers Directly
* Watch Out for Mail Hub Loops (Firewall DNS Point to Itself)

Name Server Lookup Sequence

* If I am primary or secondary for domain, return information I have or negative response
* If I have a list of “forwarders”, try forwarding the query to each IP address in that last and relay back any response
* If I do not have the “slave” option set, try asking each of the root name servers for a name server reference for the domain and then try forwarding the query to the resulting name servers and relay any response

Firewall Serving Suggestion

* Firewall Primary or Secondary Name Server for the Inside Network (Secondary Reduces Load on Firewall) and use Forwarders and Slave for Outside Net
* Automatic Configuration Via Firewall admin (GUI/TUI) Not Always Adequate
* Consider Using Explicit “Internal Mail Hub” Setting to Avoid Mail Hub Lookup Loops