1.113.5
Setup and configure basic DNS services
Weight 4

Linux Professional Institute Certification — 102

Geoffrey Robertson ge@ffrey.com

Nick Urbanik nicku@nicku.org

2005 July

Description of Objective

Candidate should be able to configure hostname lookups and troubleshoot problems with local caching-only name server. Requires an understanding of the domain registration and DNS translation process. Requires understanding key differences in configuration files for bind 4 and bind 8.

Key files, terms, and utilities include:

```
/etc/hosts
/etc/resolv.conf
/etc/nsswitch.conf
/etc/named.boot (v.4) or /etc/named.conf (v.8)
named
```

Shells, Scripting, Programming & Compiling

2.113.1 Configure and manage inetd, xinetd, and related services

2.113.2 Operate and perform basic configuration of sendmail

2.113.3 Operate and perform basic configuration of Apache

2.113.4 Properly manage the NFS, smb, and nmb daemons

2.113.5 **Setup and configure basic DNS services []**

2.113.7 Set up secure shell (OpenSSH)

Setup and Configure basic DNS services

Candidate should be able to configure hostname lookups and troubleshoot problems with local caching-only name server. Requires an understanding of the domain registration and DNS translation process. Requires understanding key differences in configuration files for bind 4 and bind 8.

Setup and Configure basic DNS services

```
/etc/hosts
/etc/resolv.conf
/etc/nsswitch.conf
/etc/named.boot (v.4) or /etc/named.conf (v.8)
named
```

DNS - DOMAIN NAME SERVICE

1The internet works with numbers not names.

- `www.abc.gov.au is really 203.2.218.61`

  2
  - DNS namespace is made up of a tree of domain names.

  3
  - At the top is root (.)

  4
  - Below this is the Top Level Domain (TLD)

  5
  - Below the TLD is the Second Level Domain.

  6
  - The Second level domain is handled by whoever 'owns' that domain

  7
  - Third & lower level domains are handled by the domain owner.

DNS - DOMAIN NAME SERVICE

1Example:

-
  ```
  node1.office.my-domain.com
  ^       ^       ^       ^
  |       |       |       |
  |       |       |       -- Top level domain
  |       |       -- Second level domain
  |       - Subdomain
  -- Hostname
  ```

  2

- Domain names are fully qualified (FQDN) when a name is specified all the way down to the hostname.

RESOLVING A NAME

1A name is resolved using the following steps:2

- – /etc/nsswitch.conf is checked to see what resolution method to use (eg: read /etc/hosts, use dns, use nis...)

  3

  – nsswitch says USE DNS:

  4Read resolv.conf to see what nameserver to use 5 Send request to nameserver and wait for response

  6

  * nsswitch says USE HOSTS

  7Lookup /etc/hosts for a matching hostname

The **nsswitch.conf** file

1This is a file that determines what mechanisms are used by the hostname library calls to resolve names. 2 The file contains lines with an identifier followed by a list of methods to use for name lookups. 3 An example:

- **passwd:** files nisplus nis

  shadow: files nisplus nis

  group: files nisplus nis

  hosts: db files dns

  4

- Note that the other entries like passwd, shadow and group are used for other applications like login and have nothing to do with DNS.

The **nsswitch.conf** file

1In the hosts line, we see that any hostname to be looked up will be done in the following order:

- 1. Use local databases file (.db files in /var/db)
  2. Read /etc/hosts
  3. Search DNS

  2

- The Search options can be one of:

```
nisplus (or nis+) - Consult NIS+ (Yellow Pages)
nis (or yp)       - Consult NIS
dns               - Use a DNS server
files             - Use local files like /etc/hosts
db                - Use local database files
compat            - Use NIS in compat mode
[NOTFOUND=return] - Stop searching and return host notfound
```

An example **nsswitch** file:

```
nisplus (or nis
passwd:     db files nisplus nis
shadow:     nisplus
group       db files nisplus nis

hosts:      db files nis dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files nis
protocols:  files nisplus
rpc:        files
services:   files nisplus

netgroup:   files nisplus

publickey:  nisplus

automount:  files nisplus
aliases:    files nisplus
```

The resolv.conf file

1This file configures how the system uses DNS. An example:

-
  ```
  search aes
  nameserver 10.27.1.10
  nameserver 10.27.1.254
  ```

  2

- The 'search' line says what to append to a non-fully qualified name: eg: ping node10 –> ping node10.aes

  3

- The nameserver lines tell the hostname routines which dns server to send requests to. (If first lookup fails, use the second, third etc)

BIND - Berkley Internet Name Domain

1Bind is just one implementation of a DNS. Bind is to DNS what Apache is to http. 2 Bind is configured with:

-
  ```
  /etc/named.conf   - For BIND V8
  /etc/named.boot   - For BIND V4
  ```

  3

- Know that there is a difference between V4 & V8.

  4

- Know how to configure V8 but not V4. (Different syntax)

BIND Configuration

- The configuration file contains subsections as follows:

  1Options → How named will operate 2 logging → What/how named will log information 3 Access Lists → Who can use named & what they can do 4 Remote Servers → Characteristics of remote servers 5 zones → Information about our defined domains

An Example Config file:

```
options {
        directory "/var/named/";
        forward only;
        forwarders {
            203.2.75.132;
            203.2.75.108;
        };
        query-source address * port 53;
```

```
        listen-on {
            10.27.1.10;
            127.0.0.1;
        };
        notify no;
};

#### The root zone ###
zone  "." {
        type hint;
        file  "named.ca";
};


#### A zone for localhost ###
zone  "0.0.127.in-addr.arpa" {
        type master;
        file  "0.0.127.in-addr.arpa.zone";
};

zone  "localhost" {
        type master;
        file  "localhost.zone";
};

### A local domain ###
zone  "1.27.10.in-addr.arpa" {
        type master;
        file  "1.27.10.in-addr.arpa.zone";
};

zone  "aes" {
        type master;
        file  "aes.zone";
};


key "key" {
        algorithm hmac-md5;
        secret "JoqlFqtncqurkhMOrrbQLYRcxSYXoNROvNTZBqWJFumleNkzOvEvTAbqpbMV";
};
```

Zone files:

1Each zone uses a file for:2

- - Hostname to IP address translations (Forward lookups) 3
  - IP to Hostname translatoins (Reverse lookups)

  4

- The names can be anything, but usually:

  5Forward file –> <domain>.zone 6 Reverse file –> <Net-IP>.in-addr.arpa

  7

- Where the Net-IP is the network part of the IP address.

Zone Records:

1Marks the start of a zone. 2 Defines the name server for a zone or subdomain 3 Define mail servers for domain 4 Defines an alias for a hostname 5 Defines the physical location of the server 6 Defines what services are found where (eg ftp, http etc) 7 Defines hostname to IP address translations (forward file) 8 Defines IP address to hostname translations (reverse file)

Example Forward file `/var/named/aes.zone`

SOA record NS record MX record CNAME record LOC record SRV record A record PTR record

```
@       IN      SOA     node10.aes.
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

@       IN      NS      node10.aes.

node5   IN      MX      10      mail
node6   IN      MX      10      mail
node4   IN      MX      10      mail
node2   IN      MX      10      mail
node10  IN      MX      10      mail
gw      IN      MX      10      mail

node10  IN      A       10.27.1.10
node2   IN      A       10.27.1.2
node4   IN      A       10.27.1.4
node5   IN      A       10.27.1.5
node6   IN      A       10.27.1.6
cds     IN      A       10.27.1.99
gw      IN      A       10.27.1.254

ns      IN      CNAME   node10
mail    IN      CNAME   node10
node-4  IN      CNAME   node4
```

Example reverse file `/var/named/1.27.10.in-addr.arpa.zone`

```
@       IN      SOA     @       root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      ns.aes.

2       IN      PTR     node2.aes.
4       IN      PTR     node4.aes.
5       IN      PTR     node5.aes.
6       IN      PTR     node6.aes.
10      IN      PTR     node10.aes.
99      IN      PTR     cds.aes.
254     IN      PTR     gw.aes.
```

Configuring a Caching only Nameserver

1A caching only nameserver is simple to setup. The first time a name is needed, a normal lookup occurs (Authorative) The next time that name is needed, it is returned from cache (Non-authorative) 2 Under /etc/named.conf in the options section, just make sure you have the following directives set:

-
```
options {
        directory "/var/named/";
        forward only;
        forwarders {
            <First DNS to query>;
            <Second DNS to query>;
        };
        listen-on {            <Your local IP address>;
            127.0.0.1;
        };
```

3

- Leave the root zone (.) and localhost entries as they are.

Testing DNS

1To test DNS, use one of the following tools:2

- - nslookup (deprecated) 3
  - dig 4
  - host

5

- To use in their simplest form, just add the hostname you wish to query as the first option to the command:

```
nslookup node16.c222
dig node16.c222
host node16.c222
```

`nslookup`

1Usage: `nslookup [option] host-to-find [-name-server]` Example:

- $ **`nslookup node2.aes -10.27.1.10`** ↩

2

- Note: nslookup is deprecated and may be removed from future releases. Consider using the 'dig' or 'host' programs instead. Run nslookup with the `-sil[ent]` option to prevent this message from appearing.

```
Server:         10.27.1.10
Address:        10.27.1.10#53

Name:   node2.aes
Address: 10.27.1.2
```

dig

1Usage: `dig [@name-server] host-to-find [query-type]` 2 Example:

- `$ dig @10.27.1.10 node2.aes ←`

```
; «» DiG 9.2.0 «» @10.27.1.10 node2.aes
;; global options:  printcmd
;; Got answer:
;; -»HEADER«- opcode: QUERY, status: NOERROR, id: 43860
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;node2.aes.                     IN      A

;; ANSWER SECTION:
node2.aes.              86400   IN      A       10.27.1.2

;; AUTHORITY SECTION:
aes.                    86400   IN      NS      node10.aes.

;; ADDITIONAL SECTION:
node10.aes.             86400   IN      A       10.27.1.10

;; Query time: 5 msec
;; SERVER: 10.27.1.10#53(10.27.1.10)
;; WHEN: Mon Sep  2 13:48:38 2002
;; MSG SIZE  rcvd: 80
```

host

1Usage: `host [option] host-to-find [name-server]` 2 Example:

- `$ host node2.aes ←`
  `node2.aes has address 10.27.1.2`

Exercise:

1Install bind on your machine:

1. `# rpm -Uvh bind-9*.rpm`

   2

2. Configure a Caching only nameserver on your machine. (Make all queries forward to 192.168.222.254)

3. Make changes to resolv.conf & nsswitch.conf as required (Default domain to use is c222)

   3

4. Start the named.

   ```
   # service named start
   ```

   4

5. Test it out with the host node16.c222 using:

   - nslookup
   - dig
   - host

   5

6. Test again this time with the host box16

   6

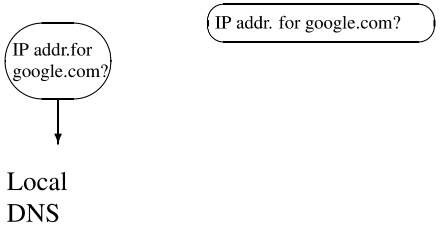
7. (For those who want a DNS challenge)

   (a) Setup a set of zones for the .c222 domain.

   (b) Insert the new zone into the main configuration file

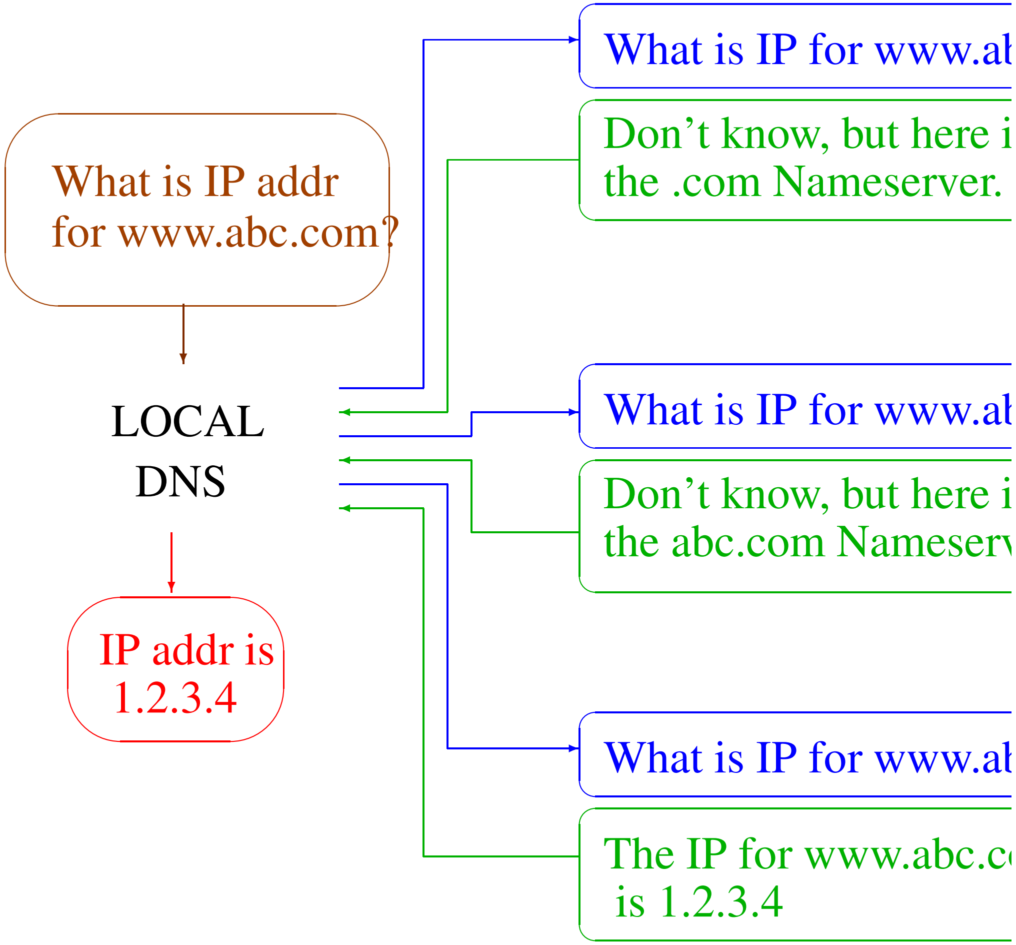
   (c) Restart the named and test it.

DNS Name Lookup Procedure



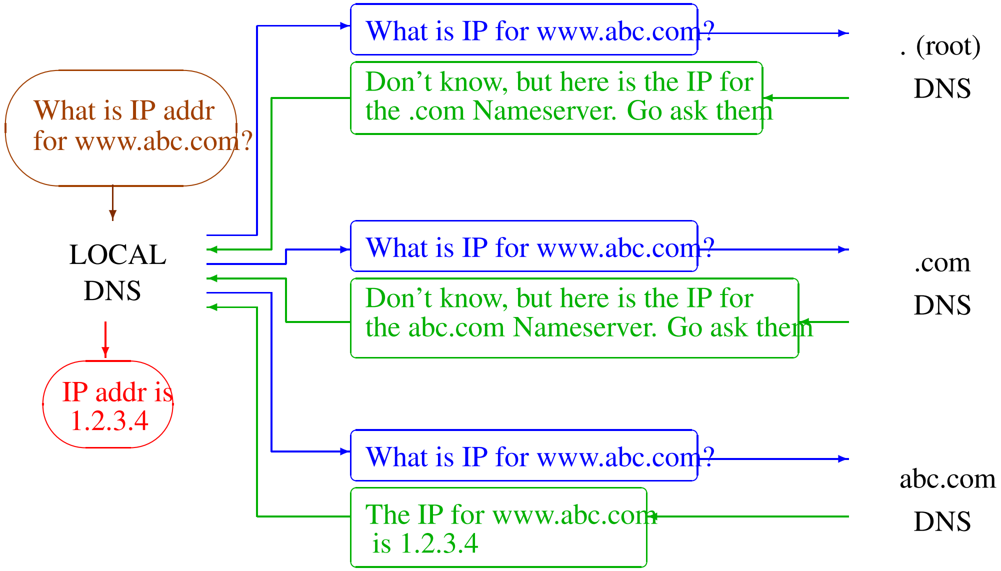
b12ah

DNS NAME LOOK



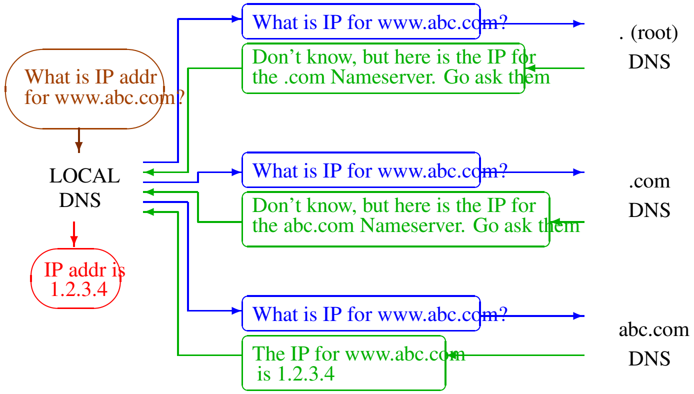
2

DNS NAME LOOKUP PROCEDURE


What is IP addr
for www.abc.com?
LOCAL
DNS
IP addr is
1.2.3.4
What is IP for www.abc.com?
Don't know, but here is the IP for
the .com Nameserver. Go ask them
. (root)
DNS
What is IP for www.abc.com?
Don't know, but here is the IP for
the abc.com Nameserver. Go ask them
.com
DNS
What is IP for www.abc.com?
The IP for www.abc.com
is 1.2.3.4
abc.com
DNS

3

DNS NAME LOOKUP PROCEDURE


What is IP addr
for www.abc.com?
LOCAL
DNS
IP addr is
1.2.3.4
What is IP for www.abc.com?
Don't know, but here is the IP for
the .com Nameserver. Go ask them
. (root)
DNS
What is IP for www.abc.com?
Don't know, but here is the IP for
the abc.com Nameserver. Go ask them
.com
DNS
What is IP for www.abc.com?
The IP for www.abc.com
is 1.2.3.4
abc.com
DNS

The End

License Of This Document