Ubuntu Server DNS

DNS Architecture and Caching Server

Introduction

- What is a DNS Infrastructure?
- How does Ubuntu (Linux) support DNS
- How is a simple Caching DNS Server setup?

What is DNS

- DNS
  - Domain Name Service
- What does it do?
  - It is a translation database
  - It maps IP Addresses to domain names
  - Given a domain name it returns the IP Address
  - (rDNS translates an IP to a domain name)

```
C:\Users\Student>nslookup www.offcampusnetwork.co.uk
Server:  www.routerlogin.com
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.offcampusnetwork.co.uk
Address:  82.133.25.41
```

Installing DNS on Ubuntu Server

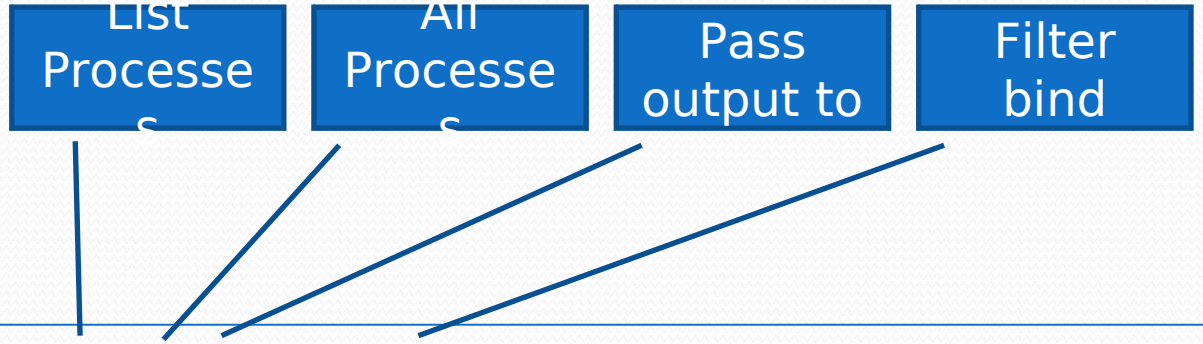
- The DNS server is in a package called **`bind9`**
- You will also require the utilities that go with the server **`dnsutils`**
- Installation of both these packages is performed using **`apt-get`**

Installing DNS on Ubuntu Server

```
student@ubuntu:~$ sudo apt-get install bind9 dnsutils
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  resolvconf rblcheck
The following NEW packages will be installed
  bind9 dnsutils
0 upgraded, 2 newly installed, 0 to remove and 41 not upgraded.
Need to get 0 B/453 kB of archives.
After this operation, 1,442 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously deselected package dnsutils.
(Reading database ... 48546 files and directories currently installed.)
Unpacking dnsutils (from .../dnsutils_1%3a9.7.3.dfsg-1ubuntu2.2_i386.deb) ...
Selecting previously deselected package bind9.
Unpacking bind9 (from .../bind9_1%3a9.7.3.dfsg-1ubuntu2.2_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for ufw ...
Processing triggers for ureadahead ...
Setting up dnsutils (1:9.7.3.dfsg-1ubuntu2.2) ...
Setting up bind9 (1:9.7.3.dfsg-1ubuntu2.2) ...
 * Starting domain name service... bind9                              [ OK ]
student@ubuntu:~$
```

Installing DNS on Ubuntu Server

- This gives a basic install of a fully functioning DNS server.
- This has very limited functionality and requires configuring before it is of any use.
- You can check to see if it running using the **ps** command

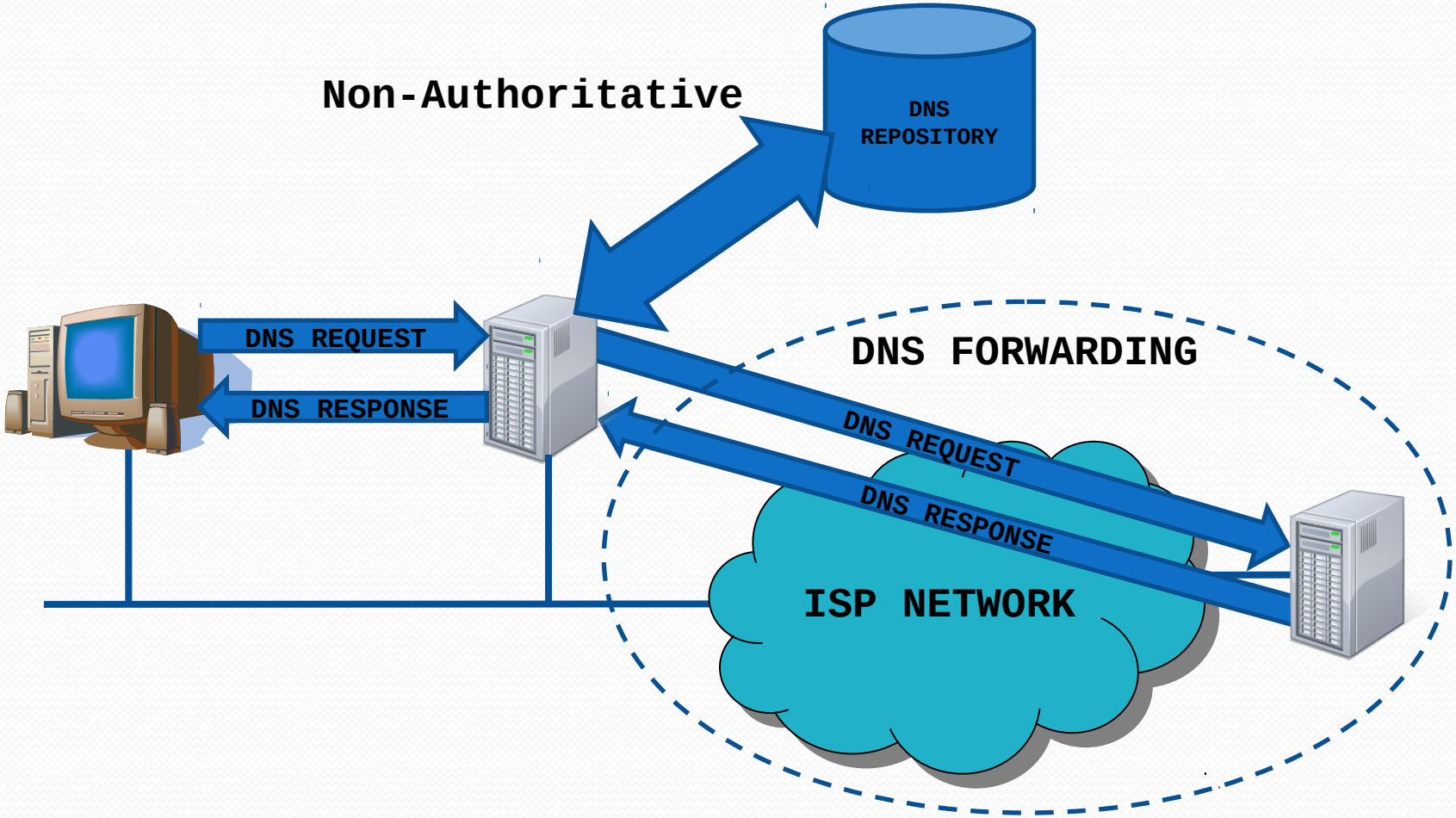



```
student@ubuntu:~$ ps -ef | grep bind
bind       635     1  0 09:10 ?        00:00:00 /usr/sbin/named -u bind
student   1097   996  0 09:15 pts/0    00:00:00 grep --color=auto bind
```

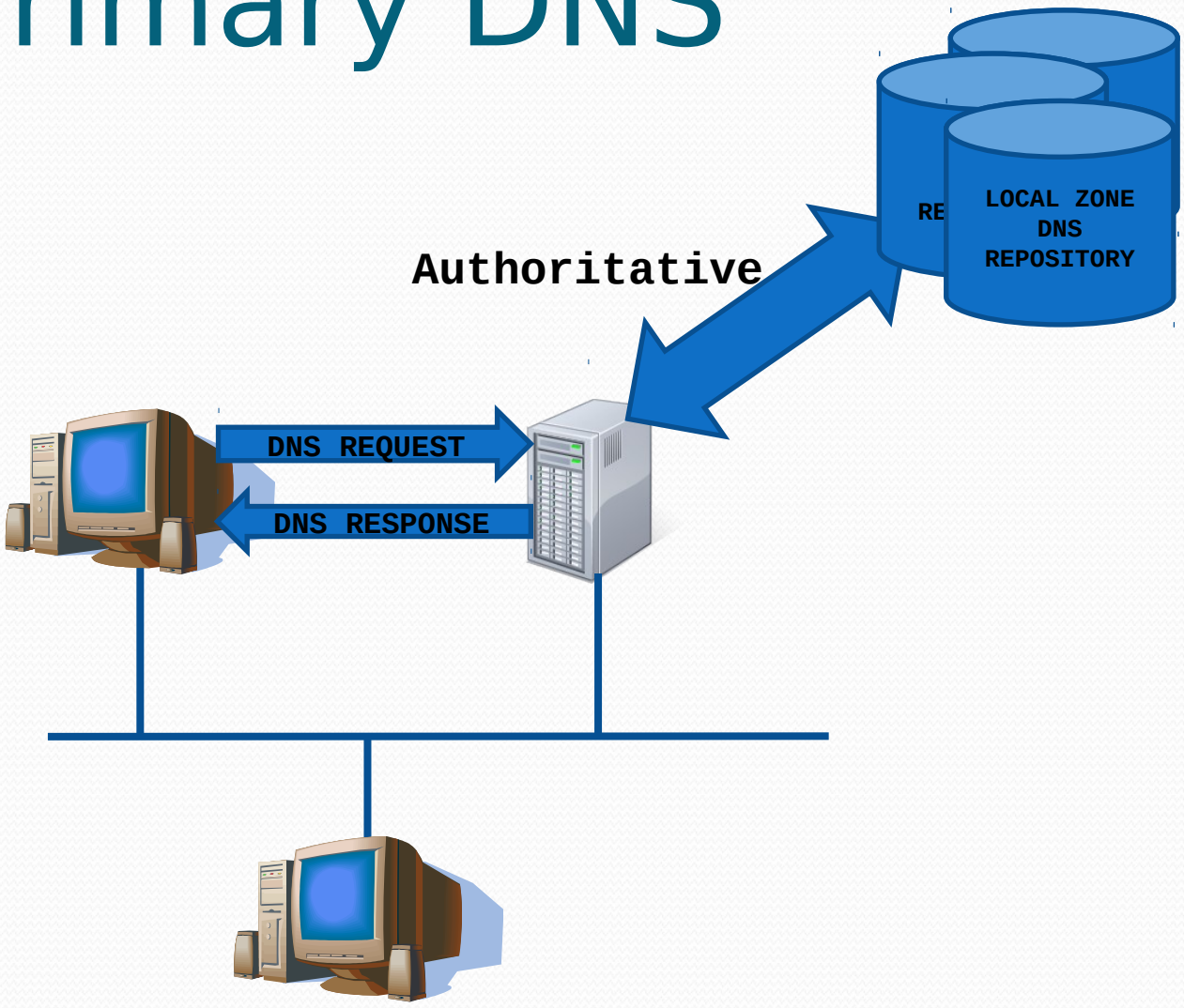
Configuring **`bind9`**

- All configuration is achieved by editing the configuration files.
- There are several ways in which to configure a DNS server
  - Caching DNS
  - Primary Master DNS
  - Secondary master DNS

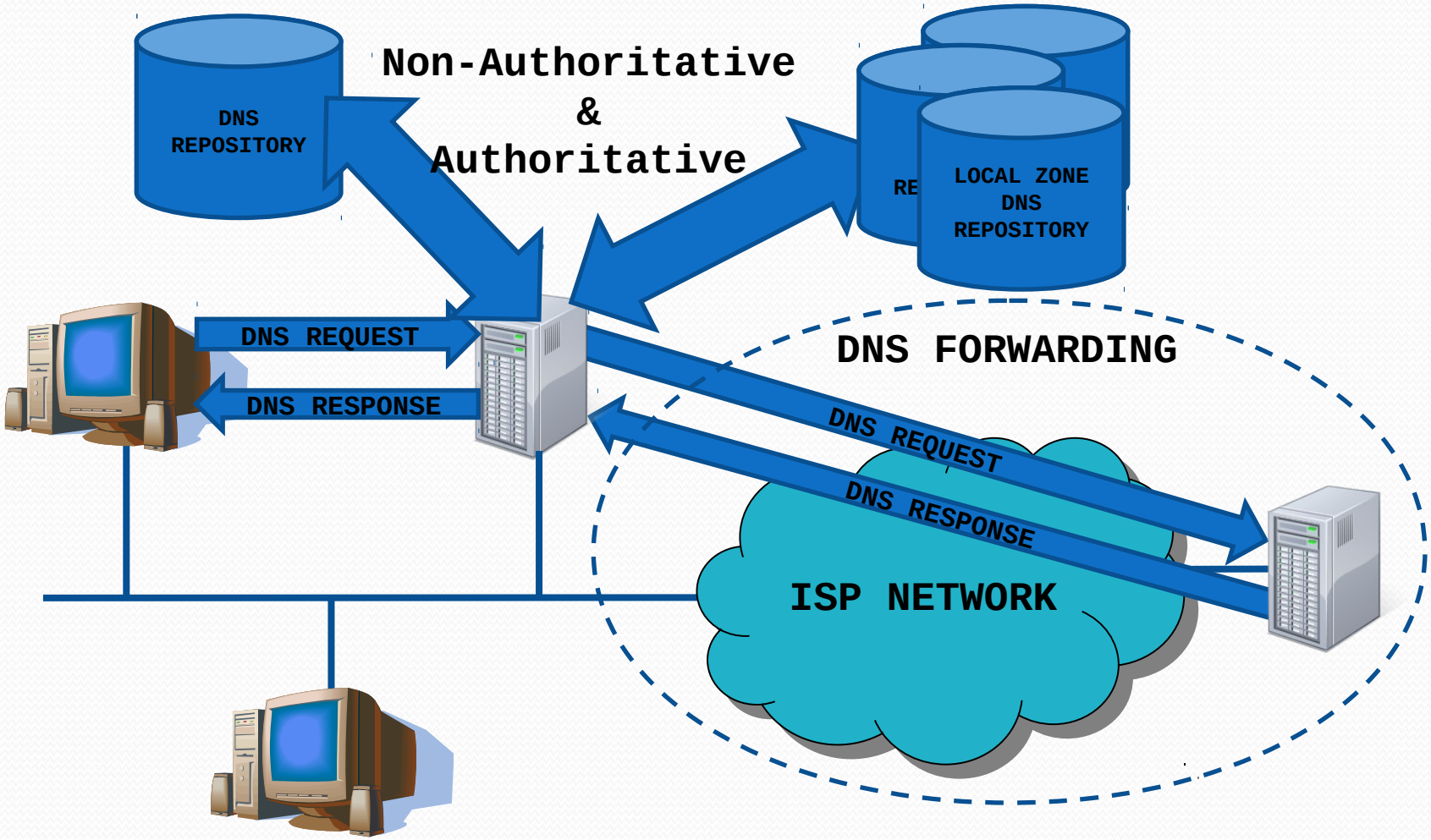
Caching DNS


Non-Authoritative
DNS REPOSITORY
DNS REQUEST
DNS RESPONSE
DNS FORWARDING
DNS REQUEST
DNS RESPONSE
ISP NETWORK

Primary DNS

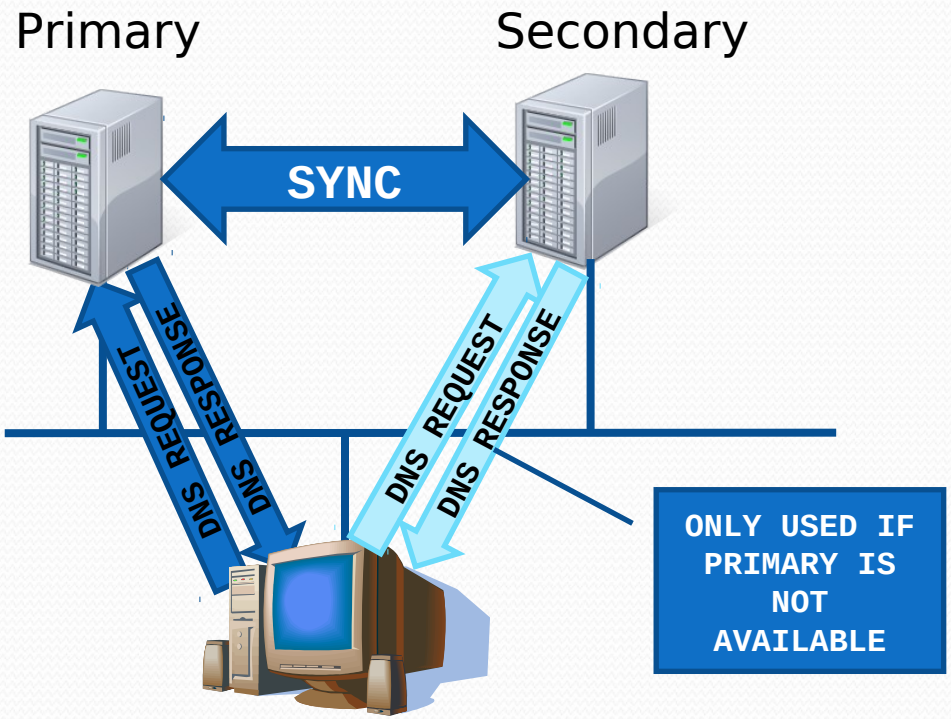

LOCAL ZONE
DNS
REPOSITORY
Authoritative
DNS REQUEST
DNS RESPONSE

Primary DNS with Caching

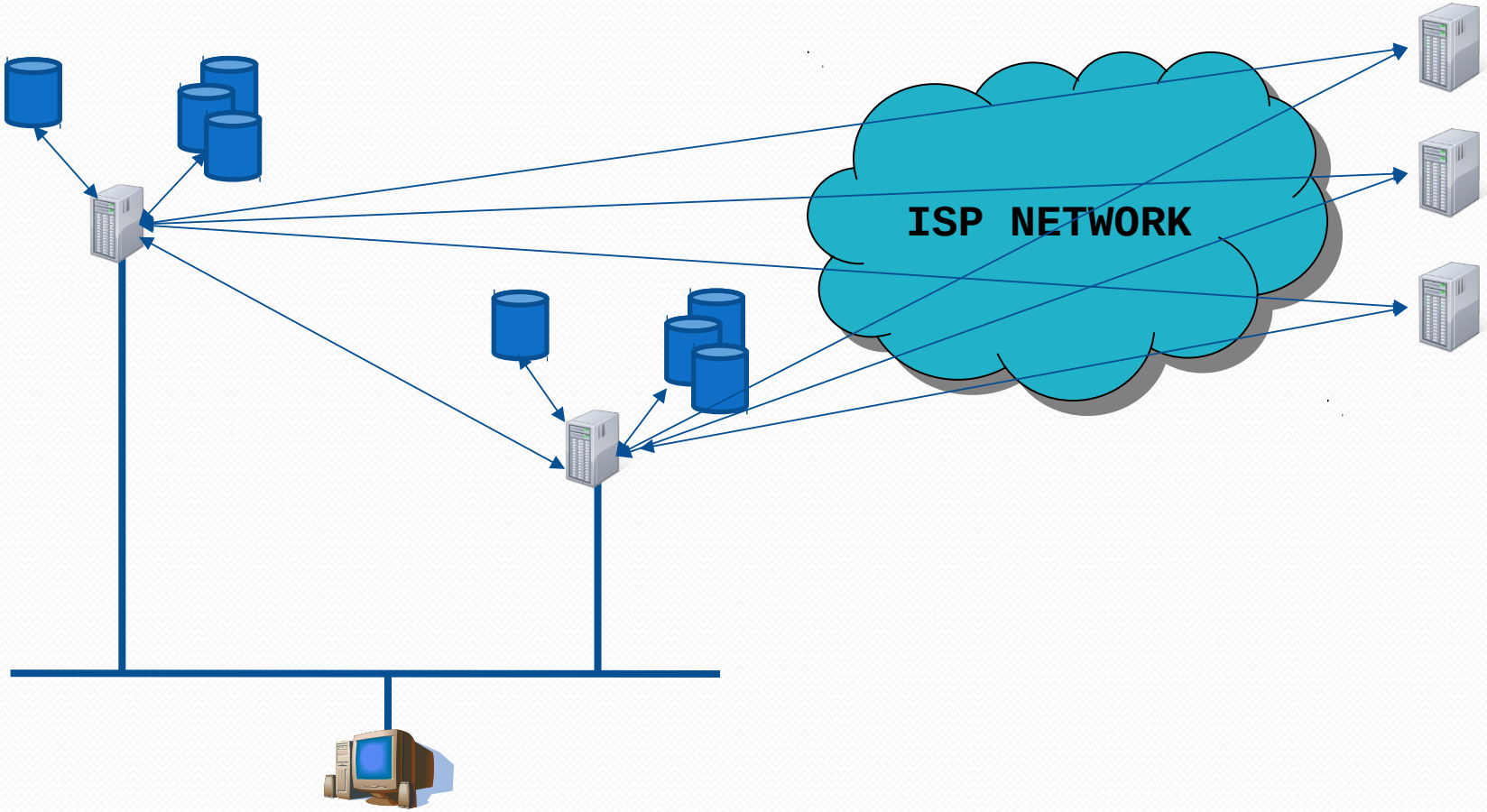


Secondary DNS

NOTE: Add the secondary DNS to your network Configuration file /etc/resolv.conf
`nameserver ?.?.?.?`



Fault Tolerant DNS



Caching DNS

- Caching DNS
  - Any query that is received will be checked against the internal database.
    - If an answer is found
      - return answer to client.
  - If not found a forward lookup will be carried out on another DNS server
    - If an answer is returned from the forwarded DNS
      - store the answer locally
      - return answer to client

Caching DNS

- Location of main configuration file.

```
/etc/bind/named.conf.options
```

Caching Server with Forwarder/s

- Default forwarding file

```
student@ubuntu:~$ pg /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

DNS Security Vulnerability

http://www.kb.cert.org/vuls/id/MIMG-7ECLCY

Ubuntu Information for VU...

Home | FAQ | Contact | Privacy Policy

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By
Name
ID Number
CVE Name
Date Public
Date Published
Date Updated
Severity Metric

Other Documents
Technical Alerts
Technical Bulletins
Alerts
Security Tips

Ubuntu Information for VU#800113

Date Notified: 2008-05-05
Date Updated: 2008-07-10
Statement Date:
Status Summary: Vulnerable

Vendor Statement

No statement is currently available from the vendor regarding this vulnerability.

Vendor Information

Vendor References

Addendum

The Ubuntu security team has published Ubuntu Security Notice USN-622-1 in response to this issue. Users are encouraged to review this notice and apply the updates it refers to.

If you have feedback, comments, or additional information about this vulnerability, please send us email.

DNS Security Vulnerability

http://www.ubuntu.com/usn/usn-622-1/

USN-622-1: Bind vulnerabili...

USN-622-1: Bind vulnerability

Ubuntu Security Notice USN-622-1

8th July, 2008

bind9 vulnerability

A security issue affects these releases of Ubuntu and its derivatives:

- Ubuntu 8.04 LTS
- Ubuntu 7.10
- Ubuntu 7.04
- Ubuntu 6.06 LTS

Software description

- bind9

Details

Dan Kaminsky discovered weaknesses in the DNS protocol as implemented by Bind. A remote attacker could exploit this to spoof DNS entries and poison DNS caches. Among other things, this could lead to misdirected email and web traffic.

Update instructions

The problem can be corrected by updating your system to the following package version:

Ubuntu 8.04 LTS:

libdns35 1:9.4.2-10ubuntu0.1

Ubuntu 7.10:

libdns32 1:9.4.1-P1-3ubuntu2

Ubuntu 7.04:

libdns22 1:9.3.4-2ubuntu2.3

Ubuntu 6.06 LTS:

libdns21 1:9.3.2-2ubuntu1.5

In general, a standard system upgrade is sufficient to effect the necessary changes.

References

CVE-2008-1447

Caching Server with Forwarder/s

- Modified forwarding file

```
student@ubuntu:~$ pg /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

           forwarders {
                   192.168.1.254;
                   192.168.1.253;
           };

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Caching Server with Forwarder/s

- Restart the DNS Server

```
$>sudo /etc/init.d/bind9 restart
```

Caching Server with Forwarder/s

- Restart the DNS Server

```
$>sudo /etc/init.d/bind9 restart
```

Conclusion

- What is the purpose of a DNS Server?
- What is a DNS Infrastructure?
- How does Ubuntu (Linux) support DNS
- How is a simple Caching DNS Server setup?