Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards - NA
- 1st minute quiz – done
- Web Calendar summary – done
- Web book pages – done
- Commands – done
- Howtos – NA
- Skills pacing - NA
- Lab – done
- Depot (VMs) – NA
- do-act8A-* uploaded – done
- Copies of test made

Course history and credits

Jim Griffin

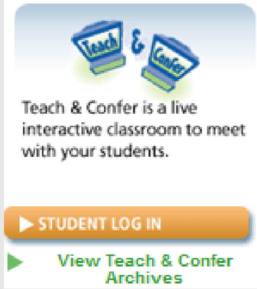
- Jim created the original version of this course
- Jim's site: http://cabrillo.edu/~jgriffin/

Rick Graziani

- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site: http://cabrillo.edu/~rgraziani/

Joe A.

Joe P.


Teach & Confer is a live interactive classroom to meet with your students.

www.cccconfer.org
dial-in: 888-886-3951
passcode: 439080

John

Junious

Robert

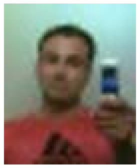
Kay

Chuck

Lieven

Rich

Jesus


Josh

Casady

Brynden

Joe B.

Chris H.

Edwin

Julio

Jack

Drew

Edgar

Ryan

Aaron

Chris B.

VMs for tonight
(**Revert**, **384MB** RAM and **power up)**
arwen celebrian
sniffer

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

No Quiz Tonight!

No quiz today since we are having a test

The Domain Name System

Objectives

- Configure both a primary Domain Name Server for a specified zone, and a secondary name server for redundancy and observing a zone transfer.

VMs for tonight
(**Revert**, **384MB** RAM and **power up**)
arwen celebrian sniffer

Agenda

- No quiz today!
- Questions on previous material
- Housekeeping
- DNS Overview
- dig command
- host command
- Forward zone database
- Reverse zone database
- named.conf
- Zone transfer
- Troubleshooting
- Demo
- Lab 7
- Wrap
- Test 2

Questions on previous material

Questions?

- Previous lesson material
- Lab assignments
- Practice test

Housekeeping

- No labs due today!

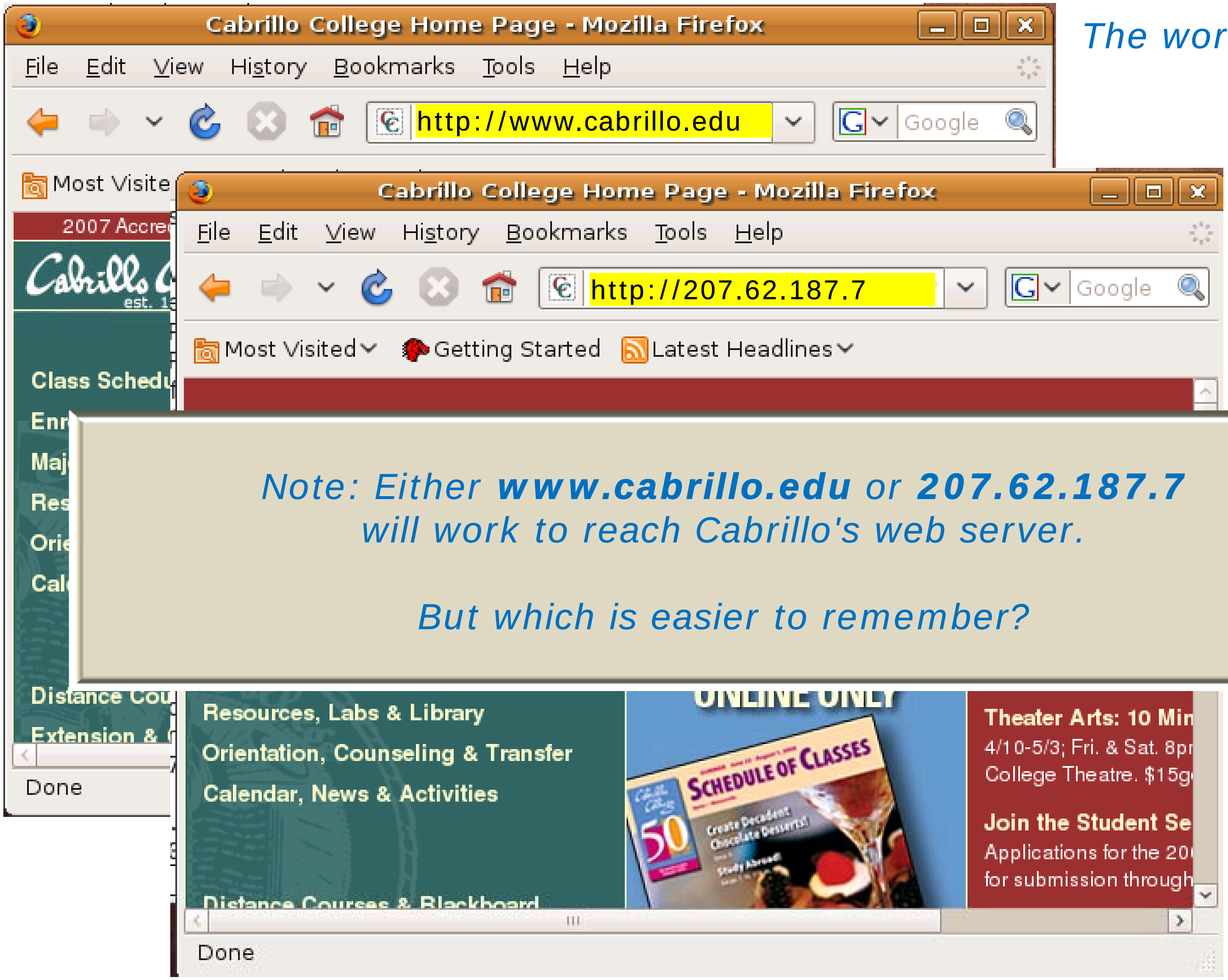
- Note you can earn up to 90 points of extra credit (labs, typos, howtos, etc.)

- Extra credit labs available:
  - X1 Permanent NIC configuration (30 points)
  - X2 PPP (30 points)
  - Original NIC lab (20 points)
  - Original routing lab (20 points)
  - Original port forwarding lab (20 points)
  - Original firewall lab (20 points)

- Weekend Lab Workshop and GAH posse
  - April 17th 1:30 - ??? (Room 2501 and 2504)

VMs for tonight
(**Revert**, **384MB** RAM and **power up**)
arwen celebrian
sniffer

DNS Overview



Cabrillo College Home Page - Mozilla Firefox

http://www.cabrillo.edu

Cabrillo College Home Page - Mozilla Firefox

http://207.62.187.7

The world with DNS

The world without DNS

*Note: Either **www.cabrillo.edu** or **207.62.187.7** will work to reach Cabrillo's web server.*

But which is easier to remember?

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Paul worked at the Information Sciences Institute of the University of Southern California

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

Can you imagine trying to keep these files updated on every single host in the world?

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
    - Primary
    - Secondary
    - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

In reality, the DNS is a huge, global distributed database spread across all the DNS servers in the world.

Each DNS server is authoritative for its own domain and maintains these forward and reverse lookup zones.

DNS - Domain Name System

Forward lookup

name to IP

```
[root@elrond]# host opus.cabrillo.edu
opus.cabrillo.edu has address 207.62.186.9
```

Reverse lookup

IP to name

```
[root@elrond]# host 207.62.186.9
9.186.62.207.in-addr.arpa domain name pointer opus.cabrillo.edu.
```

DNS works both ways

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

The client side of DNS. It initiates and sequences the queries that lead to the resolution of a name into an IP address

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Also known as the master server. This server maintains a database of hostname/IP pairs for the systems it serves. This server also provides authoritative answers for these same systems.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Also known as a slave server. This server is identical to the primary server except it does not maintain its own database. It's data is obtained instead from the primary server. Used as backup when the primary server is down and for load balancing.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Has no database of its own and does not obtain one from another server. Caching servers make queries on behalf of clients and cache the answers. Caching servers are used for performance reasons.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Contain the database resource records such as A records that map a hostname to a IP address, PTR records that map IP addresses to hostnames, NS records for name servers, and CNAME records for aliases.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

Provide either an answer or an error message

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

Provide either an answer or a referral to another DNS server

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

- Recursive
- Iterative

This is what we will install and configure in Lab 7

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the */etc/hosts* file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.*domain-name)*

Supports two type of queries:

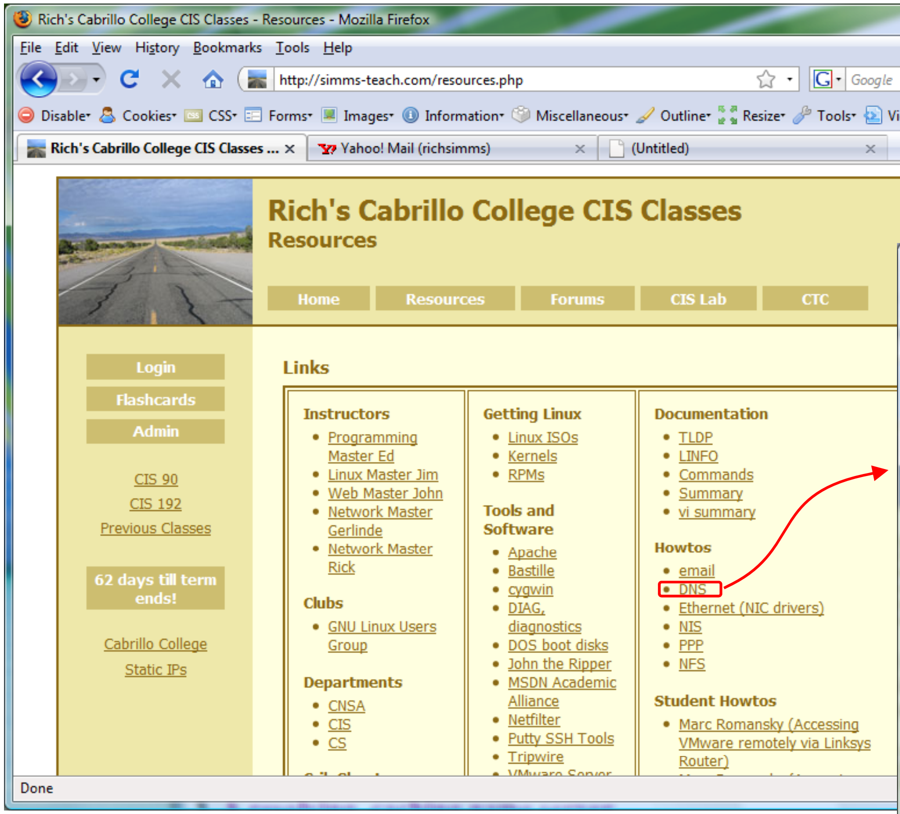
- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Software Consortium: *www.isc.org*

ISC Internet Systems Consortium

http://www.tldp.org/HOWTO/DNS-HOWTO.html


Rich's Cabrillo College CIS Classes - Resources - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://simms-teach.com/resources.php
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Op
Rich's Cabrillo College CIS Classes ...
Yahoo! Mail (richsimms)
(Untitled)
Done

Rich's Cabrillo College CIS Classes
Resources

Home | Resources | Forums | CIS Lab | CTC

Login
Flashcards
Admin

CIS 90
CIS 192
Previous Classes

62 days till term ends!

Cabrillo College
Static IPs

Links

Instructors
- Programming Master Ed
- Linux Master Jim
- Web Master John
- Network Master Gerlinde
- Network Master Rick

Clubs
- GNU Linux Users Group

Departments
- CNSA
- CIS
- CS

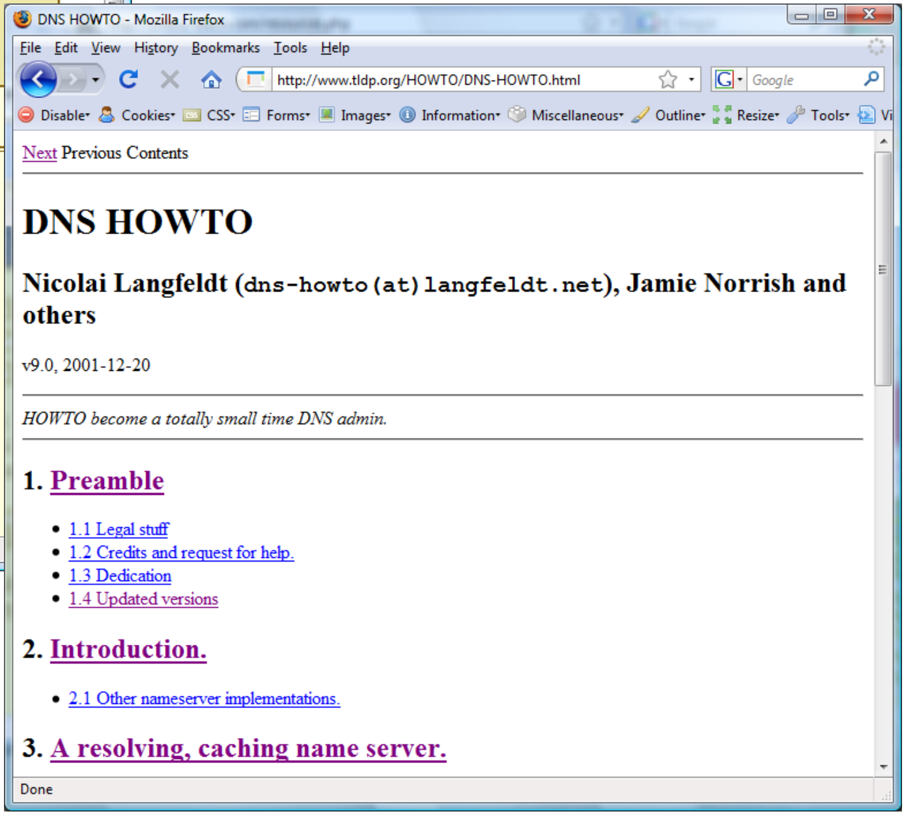
Getting Linux
- Linux ISOs
- Kernels
- RPMs

Tools and Software
- Apache
- Bastille
- cygwin
- DIAG, diagnostics
- DOS boot disks
- John the Ripper
- MSDN Academic Alliance
- Netfilter
- Putty SSH Tools
- Tripwire
- VMware Server

Documentation
- TLDP
- LINFO
- Commands
- Summary
- vi summary

Howtos
- email
- DNS
- Ethernet (NIC drivers)
- NIS
- PPP
- NFS

Student Howtos
- Marc Romansky (Accessing VMware remotely via Linksys Router)


DNS HOWTO - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.tldp.org/HOWTO/DNS-HOWTO.html
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools Vi
Done

Next Previous Contents

DNS HOWTO

Nicolai Langfeldt (dns-howto (at) langfeldt.net), Jamie Norrish and others

v9.0, 2001-12-20

HOWTO become a totally small time DNS admin.

1. Preamble

- 1.1 Legal stuff
- 1.2 Credits and request for help.
- 1.3 Dedication
- 1.4 Updated versions

2. Introduction.

- 2.1 Other nameserver implementations.

3. A resolving, caching name server.

Very good DNS reference by Nicolai Langfeldt

DNS Example

(when getting a web page)

DNS - Domain Name System

Using ARP

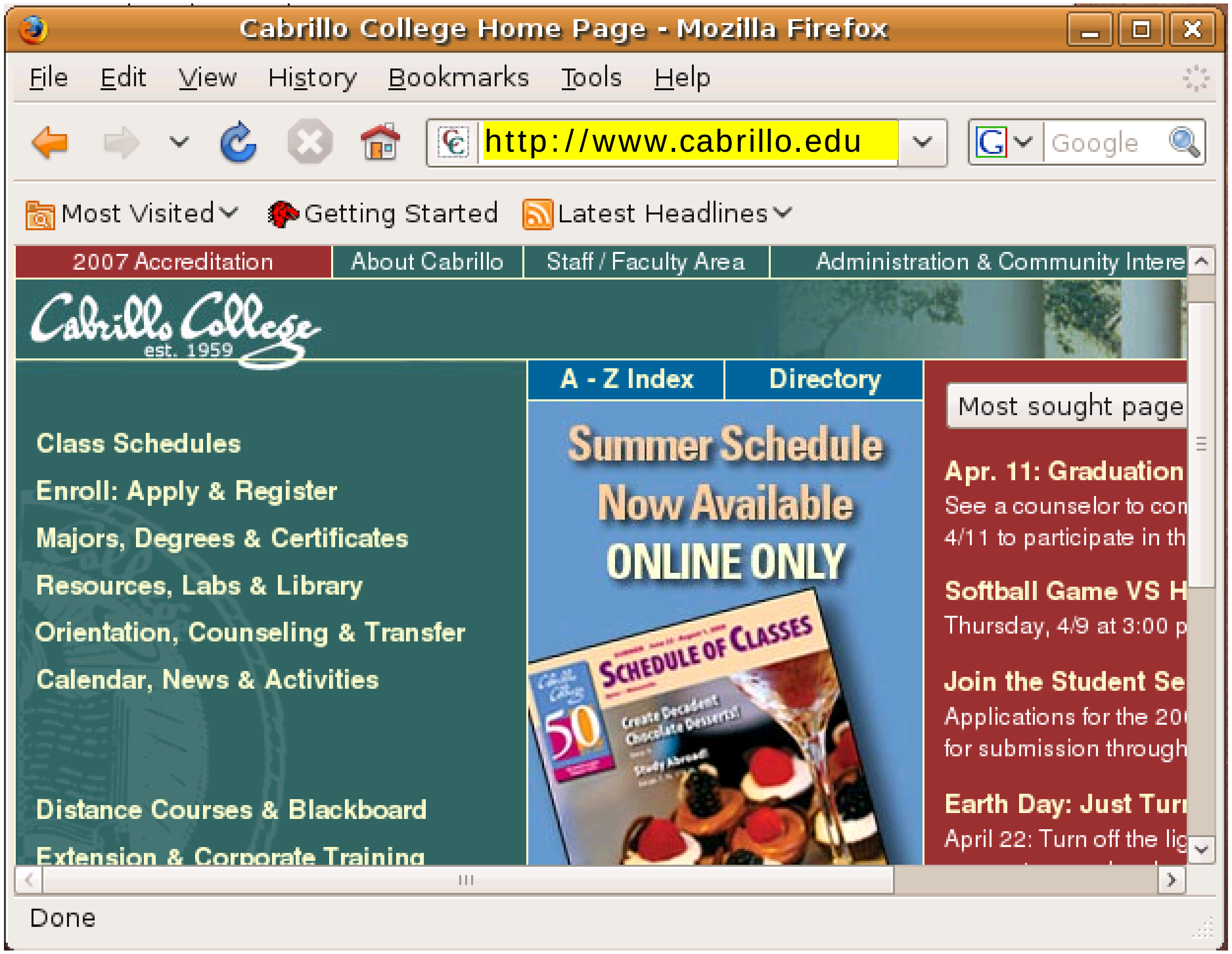
Who has this IP address?

Solution: Use ARP to get MAC address

Using DNS

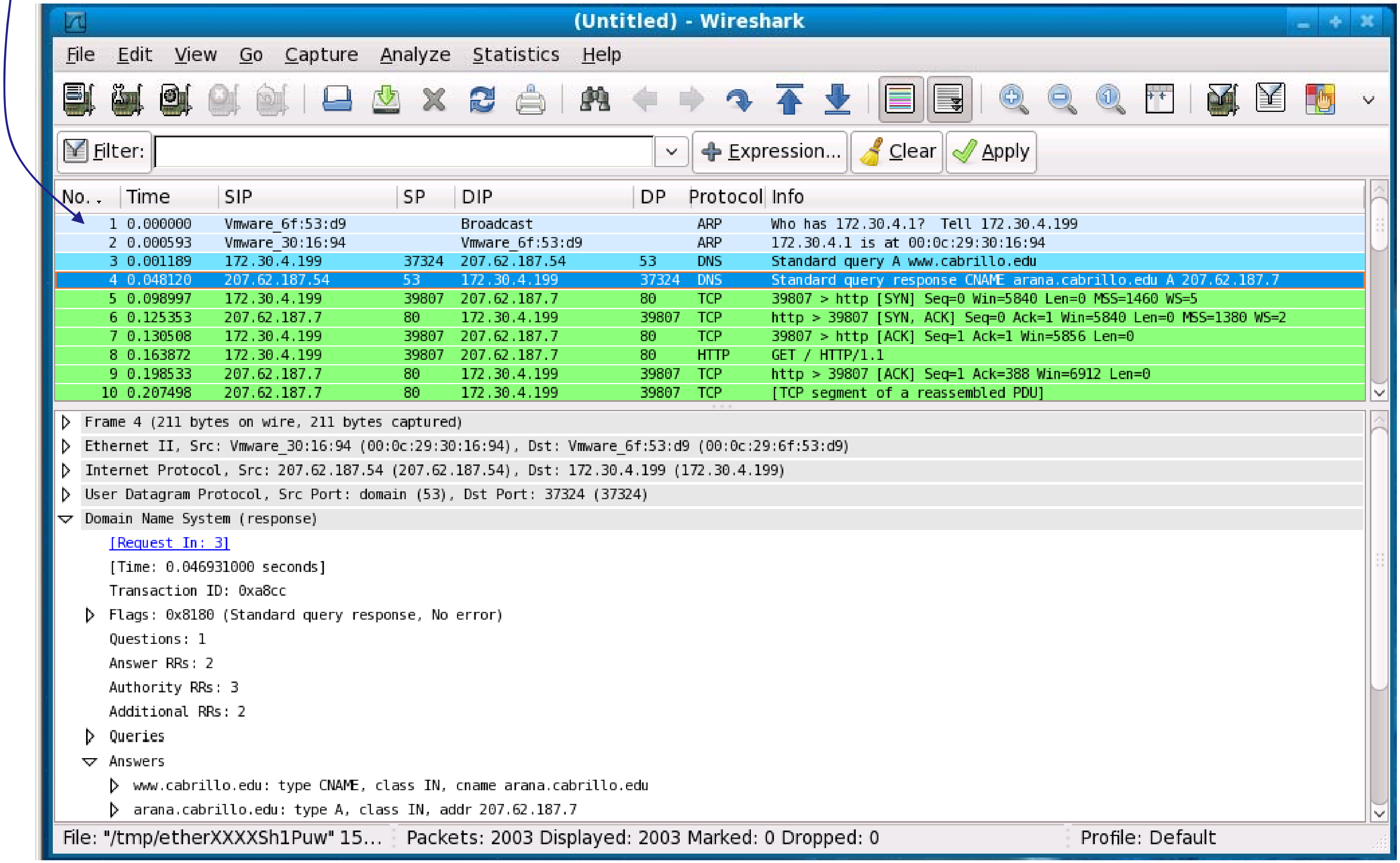
What is the IP address for this hostname?

Solution: Use DNS to resolve hostname



Lets see how DNS is used to get this web page

First, we need the MAC address of the router. This is necessary information for any packets to be sent outside the local subnet. ARP is used for this.

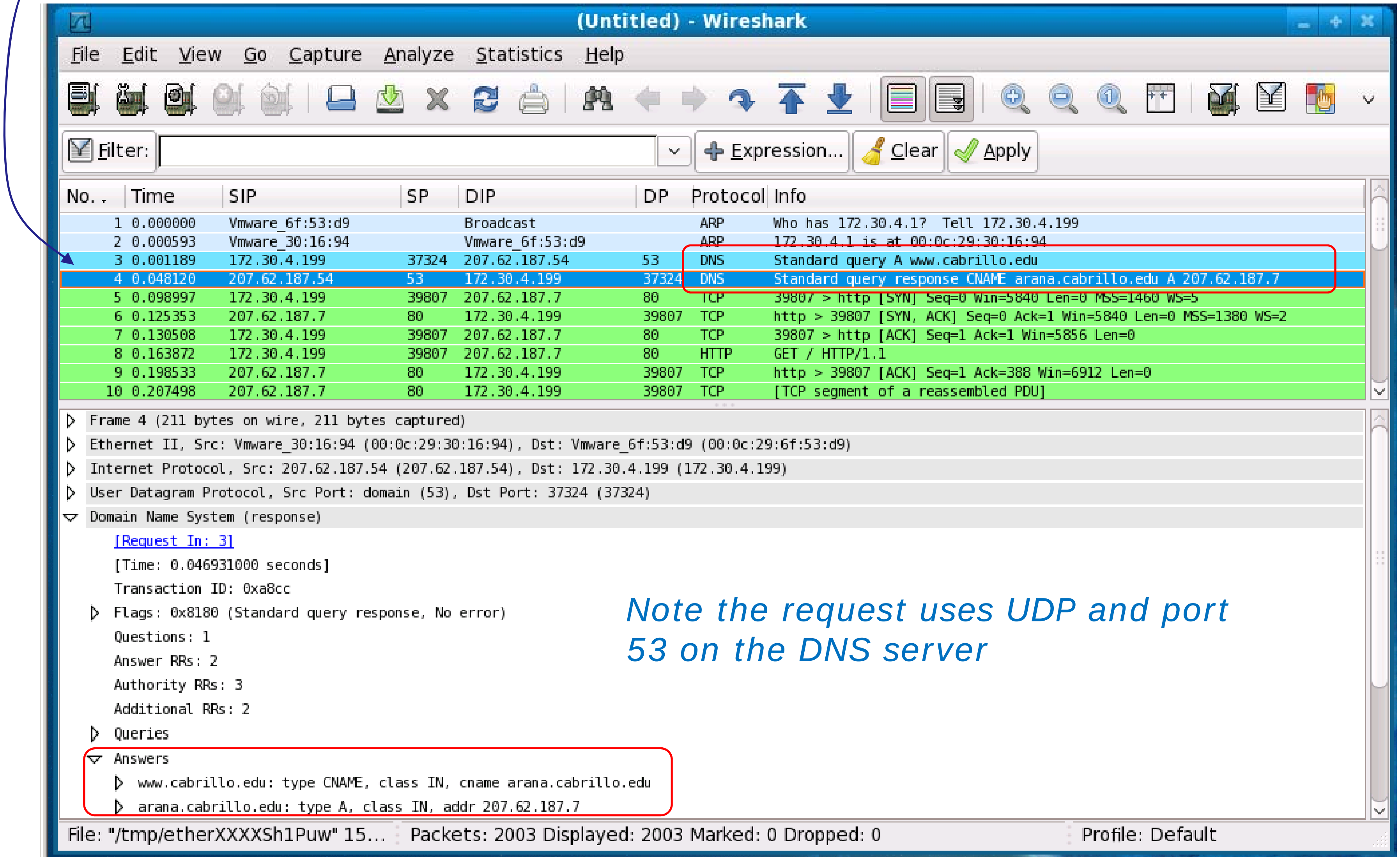


```
No. .  Time       SIP               SP     DIP               DP     Protocol Info
   1 0.000000   Vmware_6f:53:d9          Broadcast                 ARP      Who has 172.30.4.1?  Tell 172.30.4.199
   2 0.000593   Vmware_30:16:94          Vmware_6f:53:d9           ARP      172.30.4.1 is at 00:0c:29:30:16:94
   3 0.001189   172.30.4.199      37324  207.62.187.54     53     DNS      Standard query A www.cabrillo.edu
   4 0.048120   207.62.187.54     53     172.30.4.199      37324  DNS      Standard query response CNAME arana.cabrillo.edu A 207.62.187.7
   5 0.098997   172.30.4.199      39807  207.62.187.7      80     TCP      39807 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
   6 0.125353   207.62.187.7      80     172.30.4.199      39807  TCP      http > 39807 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 WS=2
   7 0.130508   172.30.4.199      39807  207.62.187.7      80     TCP      39807 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0
   8 0.163872   172.30.4.199      39807  207.62.187.7      80     HTTP     GET / HTTP/1.1
   9 0.198533   207.62.187.7      80     172.30.4.199      39807  TCP      http > 39807 [ACK] Seq=1 Ack=388 Win=6912 Len=0
  10 0.207498   207.62.187.7      80     172.30.4.199      39807  TCP      [TCP segment of a reassembled PDU]
```

```
▷ Frame 4 (211 bytes on wire, 211 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
▷ Internet Protocol, Src: 207.62.187.54 (207.62.187.54), Dst: 172.30.4.199 (172.30.4.199)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 37324 (37324)
▽ Domain Name System (response)
    [Request In: 3]
    [Time: 0.046931000 seconds]
    Transaction ID: 0xa8cc
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 2
  ▷ Queries
  ▽ Answers
    ▷ www.cabrillo.edu: type CNAME, class IN, cname arana.cabrillo.edu
    ▷ arana.cabrillo.edu: type A, class IN, addr 207.62.187.7
```

File: "/tmp/etherXXXXSh1Puw" 15... Packets: 2003 Displayed: 2003 Marked: 0 Dropped: 0 Profile: Default

Next, we send a DNS request to the server specified in /etc/resolv.conf to resolve the name www.cabrillo.edu. The answer comes back as 207.62.187.7.



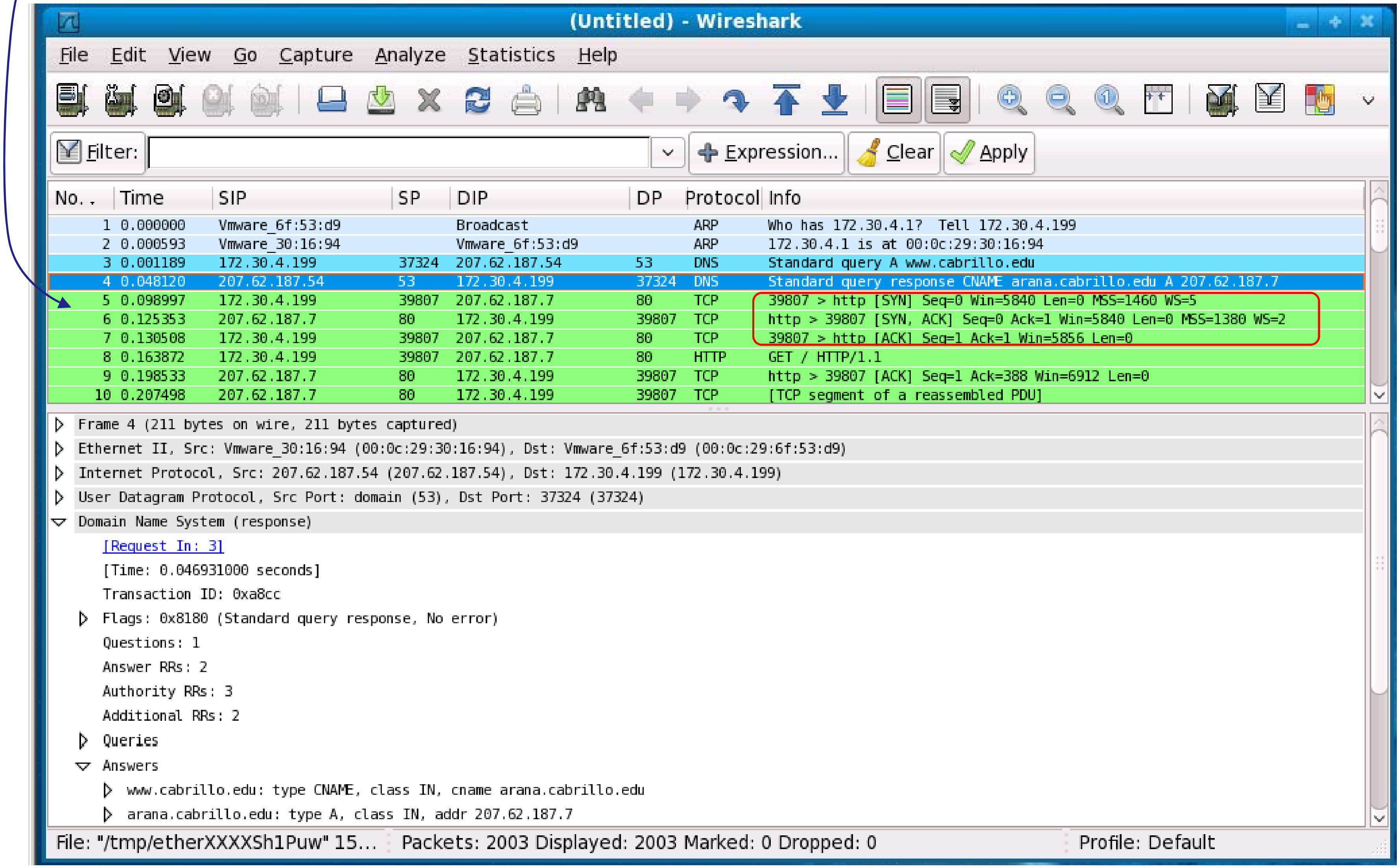
```
No. .  Time      SIP              SP     DIP              DP     Protocol Info
     1 0.000000  Vmware_6f:53:d9         Broadcast               ARP      Who has 172.30.4.1?  Tell 172.30.4.199
     2 0.000593  Vmware_30:16:94         Vmware_6f:53:d9         ARP      172.30.4.1 is at 00:0c:29:30:16:94
     3 0.001189  172.30.4.199     37324  207.62.187.54    53     DNS      Standard query A www.cabrillo.edu
     4 0.048120  207.62.187.54    53     172.30.4.199     37324  DNS      Standard query response CNAME arana.cabrillo.edu A 207.62.187.7
     5 0.098997  172.30.4.199     39807  207.62.187.7     80     TCP      39807 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
     6 0.125353  207.62.187.7     80     172.30.4.199     39807  TCP      http > 39807 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 WS=2
     7 0.130508  172.30.4.199     39807  207.62.187.7     80     TCP      39807 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0
     8 0.163872  172.30.4.199     39807  207.62.187.7     80     HTTP     GET / HTTP/1.1
     9 0.198533  207.62.187.7     80     172.30.4.199     39807  TCP      http > 39807 [ACK] Seq=1 Ack=388 Win=6912 Len=0
    10 0.207498  207.62.187.7     80     172.30.4.199     39807  TCP      [TCP segment of a reassembled PDU]
```

```
▷ Frame 4 (211 bytes on wire, 211 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
▷ Internet Protocol, Src: 207.62.187.54 (207.62.187.54), Dst: 172.30.4.199 (172.30.4.199)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 37324 (37324)
▽ Domain Name System (response)
    [Request In: 3]
    [Time: 0.046931000 seconds]
    Transaction ID: 0xa8cc
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 2
  ▷ Queries
  ▽ Answers
    ▷ www.cabrillo.edu: type CNAME, class IN, cname arana.cabrillo.edu
    ▷ arana.cabrillo.edu: type A, class IN, addr 207.62.187.7
```

File: "/tmp/etherXXXXSh1Puw" 15... Packets: 2003 Displayed: 2003 Marked: 0 Dropped: 0 Profile: Default

Note the request uses UDP and port 53 on the DNS server

Next a connection is made using with a three-way handshake with the web server

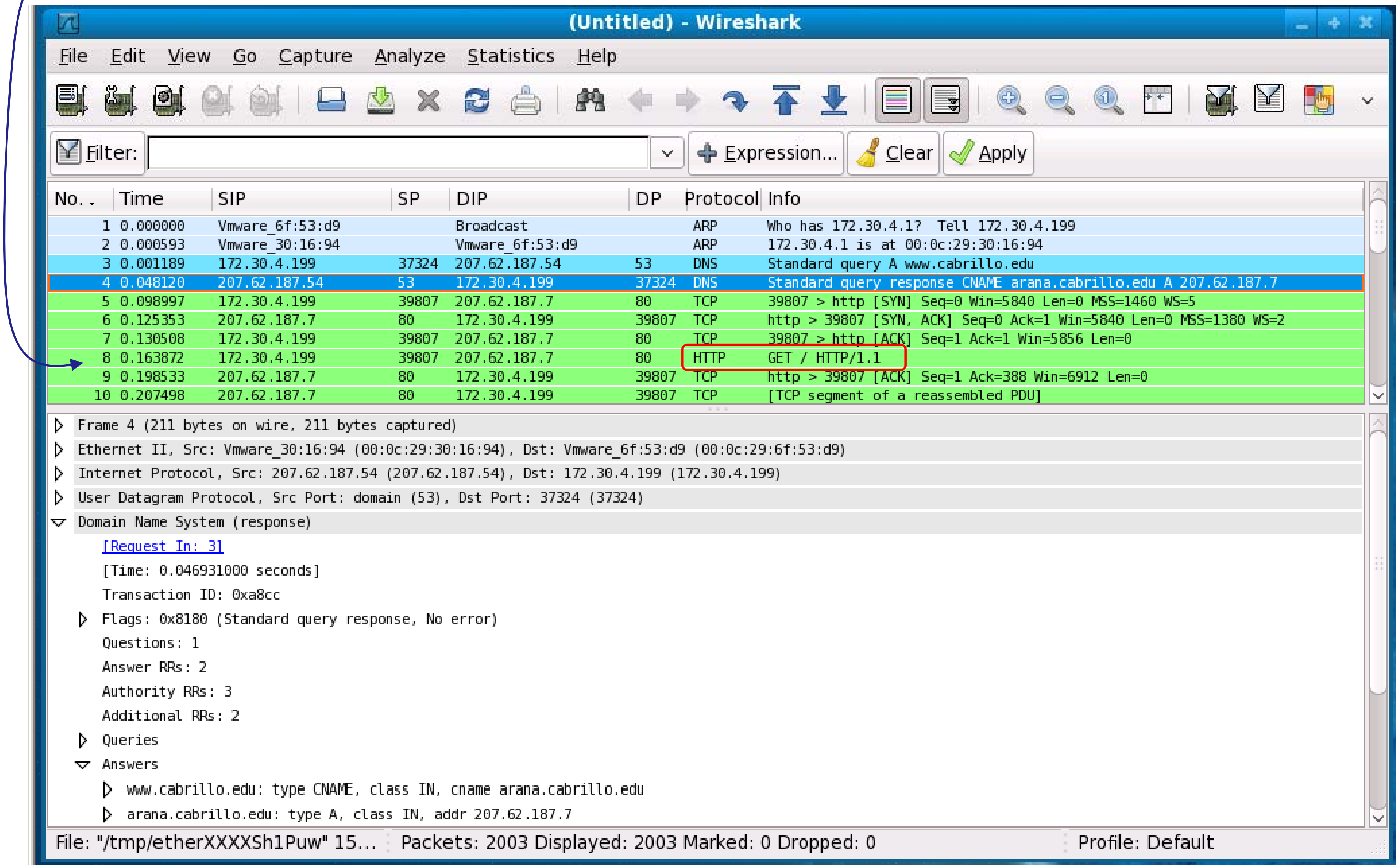


```
No. .  Time      SIP              SP     DIP              DP     Protocol Info
    1 0.000000  Vmware_6f:53:d9          Broadcast               ARP      Who has 172.30.4.1?  Tell 172.30.4.199
    2 0.000593  Vmware_30:16:94          Vmware_6f:53:d9         ARP      172.30.4.1 is at 00:0c:29:30:16:94
    3 0.001189  172.30.4.199     37324  207.62.187.54    53     DNS      Standard query A www.cabrillo.edu
    4 0.048120  207.62.187.54    53     172.30.4.199     37324  DNS      Standard query response CNAME arana.cabrillo.edu A 207.62.187.7
    5 0.098997  172.30.4.199     39807  207.62.187.7     80     TCP      39807 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
    6 0.125353  207.62.187.7     80     172.30.4.199     39807  TCP      http > 39807 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 WS=2
    7 0.130508  172.30.4.199     39807  207.62.187.7     80     TCP      39807 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0
    8 0.163872  172.30.4.199     39807  207.62.187.7     80     HTTP     GET / HTTP/1.1
    9 0.198533  207.62.187.7     80     172.30.4.199     39807  TCP      http > 39807 [ACK] Seq=1 Ack=388 Win=6912 Len=0
   10 0.207498  207.62.187.7     80     172.30.4.199     39807  TCP      [TCP segment of a reassembled PDU]
```

```
▷ Frame 4 (211 bytes on wire, 211 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
▷ Internet Protocol, Src: 207.62.187.54 (207.62.187.54), Dst: 172.30.4.199 (172.30.4.199)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 37324 (37324)
▽ Domain Name System (response)
    [Request In: 3]
    [Time: 0.046931000 seconds]
    Transaction ID: 0xa8cc
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 2
  ▷ Queries
  ▽ Answers
    ▷ www.cabrillo.edu: type CNAME, class IN, cname arana.cabrillo.edu
    ▷ arana.cabrillo.edu: type A, class IN, addr 207.62.187.7
```

```
File: "/tmp/etherXXXXSh1Puw" 15...   Packets: 2003 Displayed: 2003 Marked: 0 Dropped: 0   Profile: Default
```

And finally the actual web page is requested …



```
No. .  Time      SIP               SP     DIP               DP     Protocol Info
     1 0.000000  Vmware_6f:53:d9          Broadcast                ARP      Who has 172.30.4.1?  Tell 172.30.4.199
     2 0.000593  Vmware_30:16:94          Vmware_6f:53:d9          ARP      172.30.4.1 is at 00:0c:29:30:16:94
     3 0.001189  172.30.4.199      37324  207.62.187.54     53     DNS      Standard query A www.cabrillo.edu
     4 0.048120  207.62.187.54     53     172.30.4.199      37324  DNS      Standard query response CNAME arana.cabrillo.edu A 207.62.187.7
     5 0.098997  172.30.4.199      39807  207.62.187.7      80     TCP      39807 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
     6 0.125353  207.62.187.7      80     172.30.4.199      39807  TCP      http > 39807 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 WS=2
     7 0.130508  172.30.4.199      39807  207.62.187.7      80     TCP      39807 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0
     8 0.163872  172.30.4.199      39807  207.62.187.7      80     HTTP     GET / HTTP/1.1
     9 0.198533  207.62.187.7      80     172.30.4.199      39807  TCP      http > 39807 [ACK] Seq=1 Ack=388 Win=6912 Len=0
    10 0.207498  207.62.187.7      80     172.30.4.199      39807  TCP      [TCP segment of a reassembled PDU]
```

```
▷ Frame 4 (211 bytes on wire, 211 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
▷ Internet Protocol, Src: 207.62.187.54 (207.62.187.54), Dst: 172.30.4.199 (172.30.4.199)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 37324 (37324)
▽ Domain Name System (response)
    [Request In: 3]
    [Time: 0.046931000 seconds]
    Transaction ID: 0xa8cc
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 2
  ▷ Queries
  ▽ Answers
    ▷ www.cabrillo.edu: type CNAME, class IN, cname arana.cabrillo.edu
    ▷ arana.cabrillo.edu: type A, class IN, addr 207.62.187.7
```

```
File: "/tmp/etherXXXXSh1Puw" 15…   Packets: 2003 Displayed: 2003 Marked: 0 Dropped: 0   Profile: Default
```

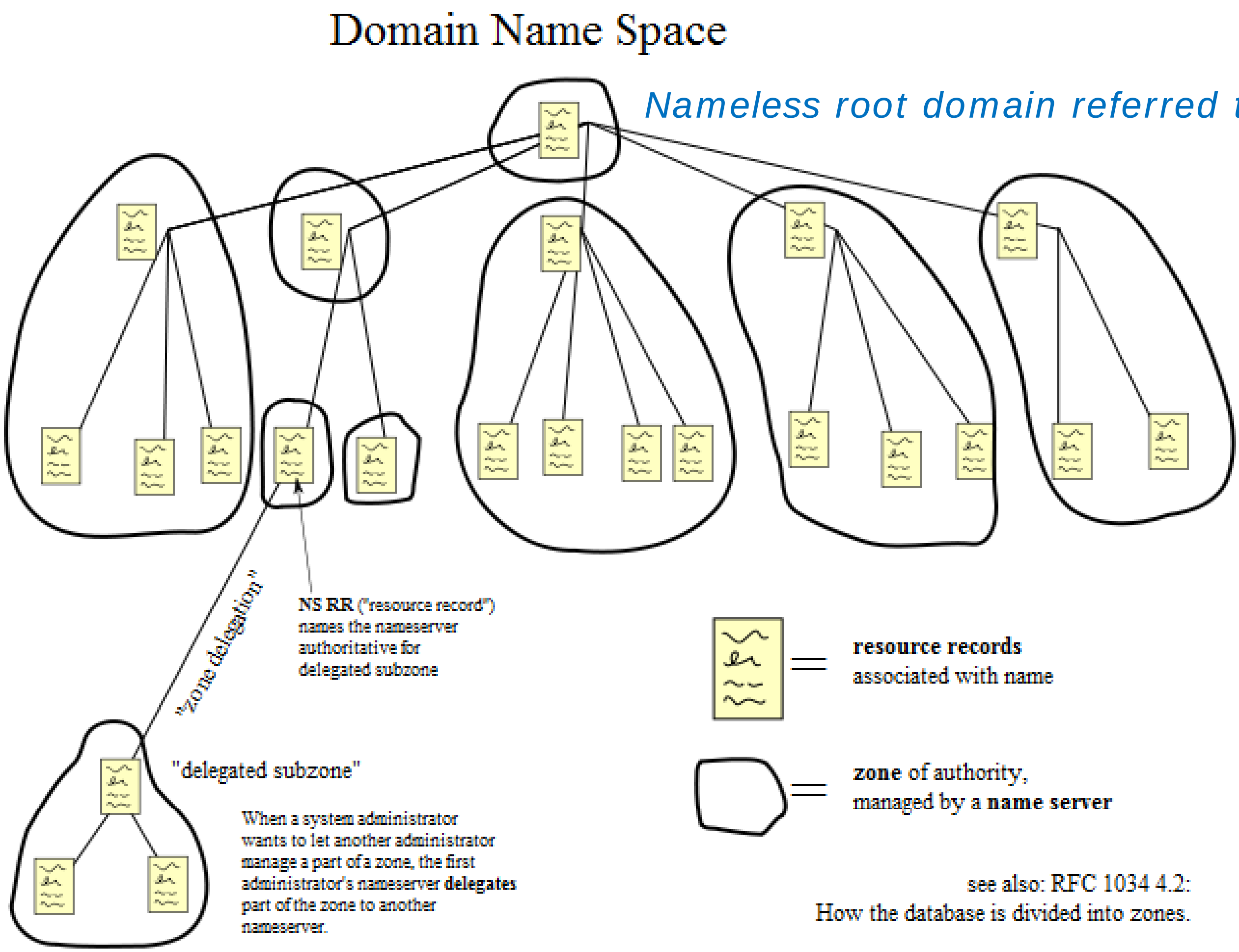
DNS Continued

The DNS Namespace

- Top most domain in the namespace hierarchy is "."
- Top-level domains: .com, .net, .gov, .edu, .org .us, ...
- Special domain for reverse lookups: *in-addr.arpa*
- Fully Qualified Domain Names read from right to left
- Name registration was handled by InterNIC; now belongs to companies for profit.

InterNIC - Internet Network Information Center. Handled domain names and IP addresses prior to 1988 before getting turned over to ICANN

ICANN - Internet Corporation for Assigned Names and Numbers. ICANN accredits the domain name registrars (the companies that compete with other and register domain names)


Domain Name Space
"zone delegation"
"delegated subzone"
resource records associated with name
zone of authority, managed by a name server

NS RR ("resource record") names the nameserver authoritative for delegated subzone

When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver **delegates** part of the zone to another nameserver.

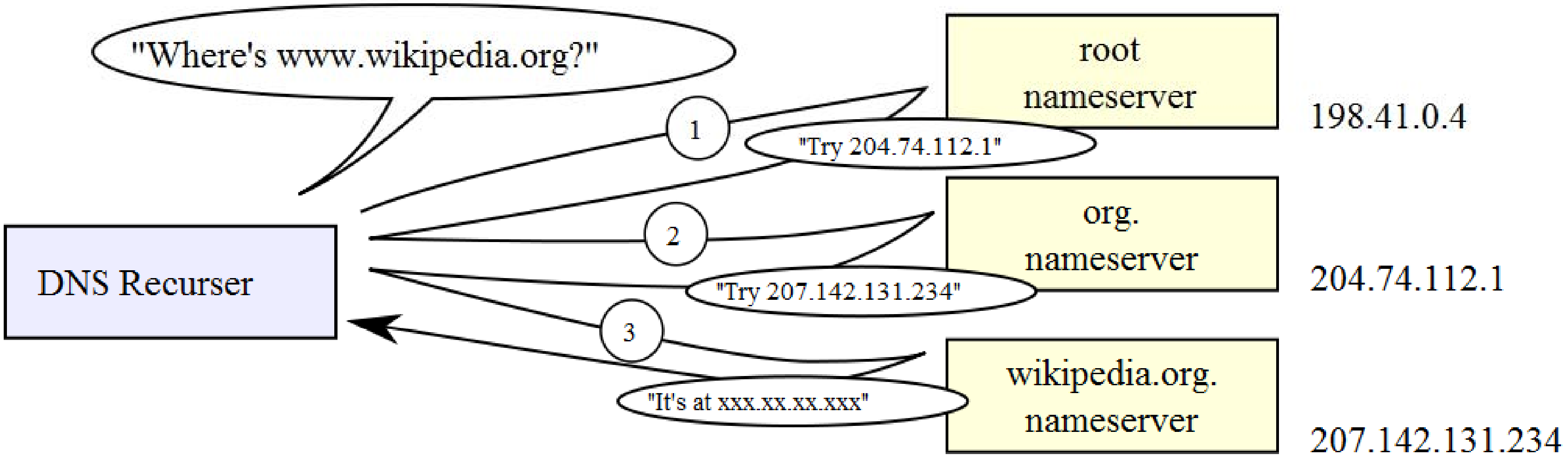
see also: RFC 1034 4.2:
How the database is divided into zones.

Nameless root domain referred to via "."

Generic TLD's - Top Level Domains (com, edu, net, org, mil, etc.)

Next level domains (e.g. hp.com, cabrillo.edu, yahoo.com, webhalks.org, etc.

source: http://en.wikipedia.org/wiki/File:Domain_name_space.svg



source: http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

One place where recursion is often used is with the local name server on a network. Rather than making client machine resolvers perform iterative resolution, it is common for the resolver to generate a recursive request to the local DNS server, which then generates iterative requests to other servers as needed. As you can see, recursive and iterative requests can be combined in a single resolution, providing significant flexibility to the process as a whole.
source: http://www.tcpipguide.com/free/t_DNSBasicNameResolutionTechniquesIterativeandRecurs-4.htm

DNS Database Resource Record types:

SOA - Start of Authority

NS - Nameserver

A - Address

PTR - Pointer (for reverse lookups)

CNAME – Aliases

MX – mail hubs

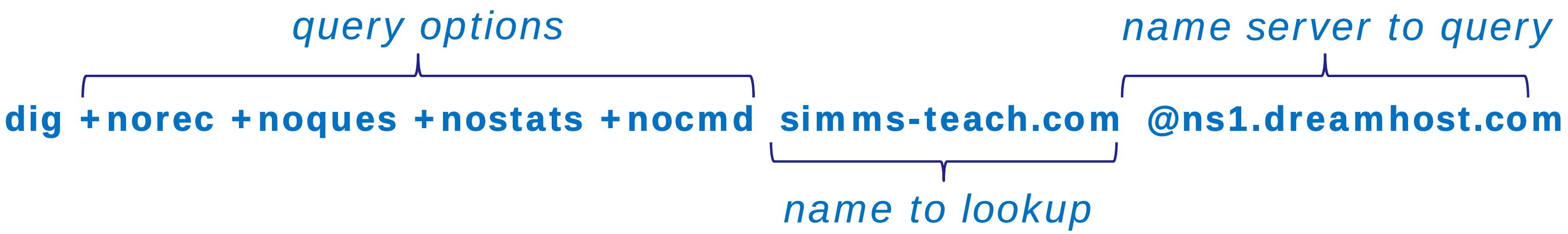
dig example

(showing manual iterative queries)

dig command

dig (domain information groper)

- Tool to interrogate DNS servers
- Performs DNS lookups and displays the answers from the DNS server queried.
- Will use name server specified in /etc/resolv.conf unless another is specified



```
dig +norec +noques +nostats +nocmd simms-teach.com @ns1.dreamhost.com
```

Some query options

+[no]recurse - [do not] use recursive queries
+[no]question - [do not] print question section when an answer is returned
+[no]stats - [do not] print query statistics
+[no]cmd - [do not] print dig version information
... for more, use **man dig**

An example of what life is like as a resolver doing a forward lookup

(using the dig command)

dig opus.cabrillo.edu (start with root "." servers)

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd opus.cabrillo.edu
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19571
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 13

;; AUTHORITY SECTION:
.                       3600000 IN      NS      A.ROOT-SERVERS.NET.
.                       3600000 IN      NS      L.ROOT-SERVERS.NET.
.                       3600000 IN      NS      I.ROOT-SERVERS.NET.
.                       3600000 IN      NS      E.ROOT-SERVERS.NET.
.                       3600000 IN      NS      D.ROOT-SERVERS.NET.
.                       3600000 IN      NS      F.ROOT-SERVERS.NET.
.                       3600000 IN      NS      B.ROOT-SERVERS.NET.
.                       3600000 IN      NS      M.ROOT-SERVERS.NET.
.                       3600000 IN      NS      J.ROOT-SERVERS.NET.
.                       3600000 IN      NS      G.ROOT-SERVERS.NET.
.                       3600000 IN      NS      K.ROOT-SERVERS.NET.
.                       3600000 IN      NS      H.ROOT-SERVERS.NET.
.                       3600000 IN      NS      C.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
B.ROOT-SERVERS.NET.     604794  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     604761  IN      A       192.33.4.12
E.ROOT-SERVERS.NET.     604794  IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     604791  IN      A       192.5.5.241
F.ROOT-SERVERS.NET.     604794  IN      AAAA    2001:500:2f::f
G.ROOT-SERVERS.NET.     604794  IN      A       192.112.36.4
I.ROOT-SERVERS.NET.     604794  IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     604794  IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     604794  IN      A       193.0.14.129
K.ROOT-SERVERS.NET.     604791  IN      AAAA    2001:7fd::1
L.ROOT-SERVERS.NET.     604794  IN      AAAA    2001:500:3::42
M.ROOT-SERVERS.NET.     604794  IN      A       202.12.27.33
M.ROOT-SERVERS.NET.     604791  IN      AAAA    2001:dc3::35

[root@elrond ~]#
```

We don't get an answer but we do get referred to a long list of root name servers we can ask.

Pick one at random to continue

IP addresses for these servers

dig opus.cabrillo.edu (edu. servers)

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd opus.cabrillo.edu @J.ROOT-SERVERS.NET.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53616
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 7, ADDITIONAL: 8

;; AUTHORITY SECTION:
edu.                    172800  IN      NS      E.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      F.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      G.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      L.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      A.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      C.GTLD-SERVERS.NET.
edu.                    172800  IN      NS      D.GTLD-SERVERS.NET.

;; ADDITIONAL SECTION:
A.GTLD-SERVERS.NET.     172800  IN      A       192.5.6.30
A.GTLD-SERVERS.NET.     172800  IN      AAAA    2001:503:a83e::2:30
C.GTLD-SERVERS.NET.     172800  IN      A       192.26.92.30
D.GTLD-SERVERS.NET.     172800  IN      A       192.31.80.30
E.GTLD-SERVERS.NET.     172800  IN      A       192.12.94.30
F.GTLD-SERVERS.NET.     172800  IN      A       192.35.51.30
G.GTLD-SERVERS.NET.     172800  IN      A       192.42.93.30
L.GTLD-SERVERS.NET.     172800  IN      A       192.41.162.30

[root@elrond ~]#
```

Still no answer but we get referred to a list of generic top level domain name servers for the edu domain

Pick one at random to continue

IP addresses for the edu domain nameservers

dig opus.cabrillo.edu (cabrillo.edu. servers)

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd opus.cabrillo.edu @F.GTLD-SERVERS.NET.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17333
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 3

;; AUTHORITY SECTION:
cabrillo.edu.           172800  IN      NS      buttercup.cabrillo.edu.
cabrillo.edu.           172800  IN      NS      ns1.csu.net.
cabrillo.edu.           172800  IN      NS      ns2.csu.net.

;; ADDITIONAL SECTION:
buttercup.cabrillo.edu. 172800  IN      A       207.62.187.54
ns1.csu.net.            172800  IN      A       130.150.102.100
ns2.csu.net.            172800  IN      A       130.150.102.20

[root@elrond ~]#
```

Still no answer but we get referred to a list of cabrillo name servers for the cabrillo.edu domain

Pick one at random to continue

IP addresses for the Cabrillo name servers

dig opus.cabrillo.edu (resolved)

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd opus.cabrillo.edu @ns1.csu.net.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6591
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; ANSWER SECTION:
opus.cabrillo.edu.      300     IN      A       207.62.186.9

;; AUTHORITY SECTION:
cabrillo.edu.           300     IN      NS      ns1.csu.net.
cabrillo.edu.           300     IN      NS      ns2.csu.net.
cabrillo.edu.           300     IN      NS      buttercup.cabrillo.edu.

;; ADDITIONAL SECTION:
ns1.csu.net.            15219   IN      A       130.150.102.100
ns2.csu.net.            15324   IN      A       130.150.102.20
buttercup.cabrillo.edu. 300     IN      A       207.62.187.54

[root@elrond ~]#
```

Hooray! It worked …. we got an answer!

host command

host command

Forward lookup

```
[root@elrond named]# host www.google.com
www.google.com is an alias for www.l.google.com.
www.l.google.com has address 74.125.127.99
www.l.google.com has address 74.125.127.103
www.l.google.com has address 74.125.127.104
www.l.google.com has address 74.125.127.147
```

Reverse lookup

```
[root@elrond named]# host 74.125.127.99
99.127.125.74.in-addr.arpa domain name pointer pz-in-f99.google.com.
[root@elrond named]#
```

Note the structure of the IP address "hostname" (reverse order with top of tree on the right and leaves to the left)

DNS Service Installation

DNS Installation and Configuration

Package names:	bind, caching-nameserver	
Daemon name:	/usr/sbin/named	
Startup script:	/etc/rc.d/init.d/named start or **service named start**	
Database files:	/var/named/named.ca	*IP address of root servers*
	/var/named/db.*in-addr.arpa*	*reverse lookups*
	/var/named/db.*domain-name*	*forward lookups*
Configuration files:	/etc/named.conf	*Overall configuration file*
	/etc/resolv.conf	*DNS server to use*
	/etc/nsswitch.conf	*Lookup order definition*

To reload configuration files: **rndc reload**

Service Applications

Steps to installing services

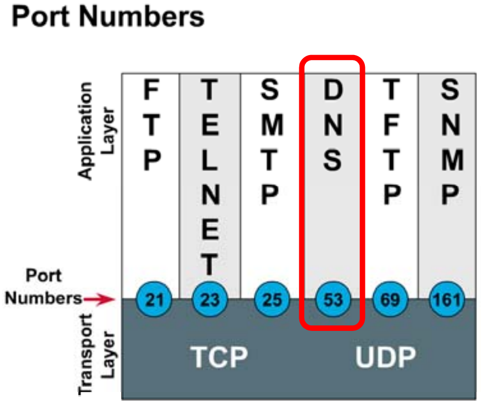
1. Install software package using **yum**, **rpm** or build from source code
2. Customize service's configuration file
3. Modify the firewall to allow access to the service
4. Customize SELinux context settings to allow use
5. Start the service
6. Configure service to automatically start when system boots
7. Monitor and verify service is running
8. Troubleshoot as necessary
9. Monitor log files as appropriate
10. Configure additional security

Installing and Configuring DNS Service (Red Hat Family)

DNS

- Resolves names like “opus.cabrillo.edu” to IP addresses
- Client-server model
- Uses port 53
- “named” – the name of the daemon (service)
- “bind” – the name of the DNS package

```
[root@elrond bin]# cat /etc/services | grep -w 53
domain          53/tcp              # name-domain server
domain          53/udp
[root@elrond bin]#
```



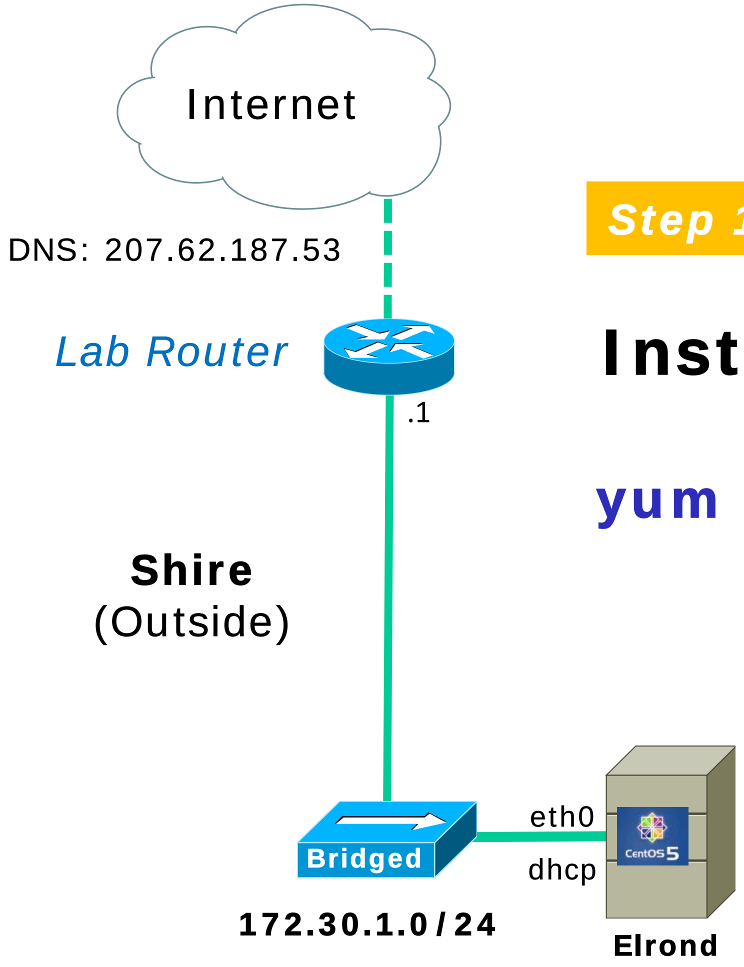
Installing and Configuring DNS Service
(Red Hat Family)

Is it installed?

```
[root@elrond bin]# rpm -qa | grep bind
bind-utils-9.3.6-4.P1.el5_4.2
ypbind-1.19-12.el5
bind-libs-9.3.6-4.P1.el5_4.2
bind-9.3.6-4.P1.el5_4.2
[root@elrond bin]# rpm -qa | grep caching-nameserver
caching-nameserver-9.3.6-4.P1.el5_4.2
[root@elrond bin]#
```

The highlighted packages above are require to install the DNS service.

Installing Software Package (using yum)



Step 1 *Installing service with yum*

Installing DNS service

yum install bind caching-nameserver

Internet connection is required for yum installs

Installing Software Package (using yum)

```
[root@elrond ~]# yum install bind caching-nameserver
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * addons: mirror.5ninesolutions.com
 * base: ftp.osuosl.org
 * extras: mirrors.liquidweb.com
 * updates: mirror.nwresd.org
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package bind.i386 30:9.3.6-4.P1.el5_4.2 set to be updated
--> Processing Dependency: bind-libs = 30:9.3.6-4.P1.el5_4.2 for package: bind
---> Package caching-nameserver.i386 30:9.3.6-4.P1.el5_4.2 set to be updated
--> Running transaction check
--> Processing Dependency: bind-libs = 30:9.3.6-4.P1.el5 for package: bind-utils
---> Package bind-libs.i386 30:9.3.6-4.P1.el5_4.2 set to be updated
--> Running transaction check
---> Package bind-utils.i386 30:9.3.6-4.P1.el5_4.2 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

Note that bind has two dependencies: bind-libs and bind-utils

Installing Software Package (using yum)

```
================================================================================
 Package                Arch     Version                      Repository   Size
================================================================================
Installing:
 bind                   i386     30:9.3.6-4.P1.el5_4.2        updates     978 k
 caching-nameserver     i386     30:9.3.6-4.P1.el5_4.2        updates      61 k
Updating for dependencies:
 bind-libs              i386     30:9.3.6-4.P1.el5_4.2        updates     857 k
 bind-utils             i386     30:9.3.6-4.P1.el5_4.2        updates     170 k

Transaction Summary
================================================================================
Install      2 Package(s)
Update       2 Package(s)
Remove       0 Package(s)

Total download size: 2.0 M
Is this ok [y/N]: y
Downloading Packages:
(1/4): caching-nameserver-9.3.6-4.P1.el5_4.2.i386.rpm    |  61 kB     00:01
(2/4): bind-utils-9.3.6-4.P1.el5_4.2.i386.rpm            | 170 kB     00:01
(3/4): bind-libs-9.3.6-4.P1.el5_4.2.i386.rpm             | 857 kB     00:05
(4/4): bind-9.3.6-4.P1.el5_4.2.i386.rpm                  | 978 kB     00:06
--------------------------------------------------------------------------------
Total                                           130 kB/s | 2.0 MB     00:15
```

Note that bind has two dependencies: bind-libs and bind-utils

Installing Software Package (using yum)

```
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating       : bind-libs                                                1/6
  Installing     : bind                                                     2/6
  Installing     : caching-nameserver                                       3/6
  Updating       : bind-utils                                               4/6
  Cleanup        : bind-libs                                                5/6
  Cleanup        : bind-utils                                               6/6

Installed:
  bind.i386 30:9.3.6-4.P1.el5_4.2 caching-nameserver.i386 30:9.3.6-4.P1.el5_4.2

Dependency Updated:
  bind-libs.i386 30:9.3.6-4.P1.el5_4.2   bind-utils.i386 30:9.3.6-4.P1.el5_4.2

Complete!
```

Installing Software Package (using rpm)

Elrond

Step 1
alternative

Installing service with rpm

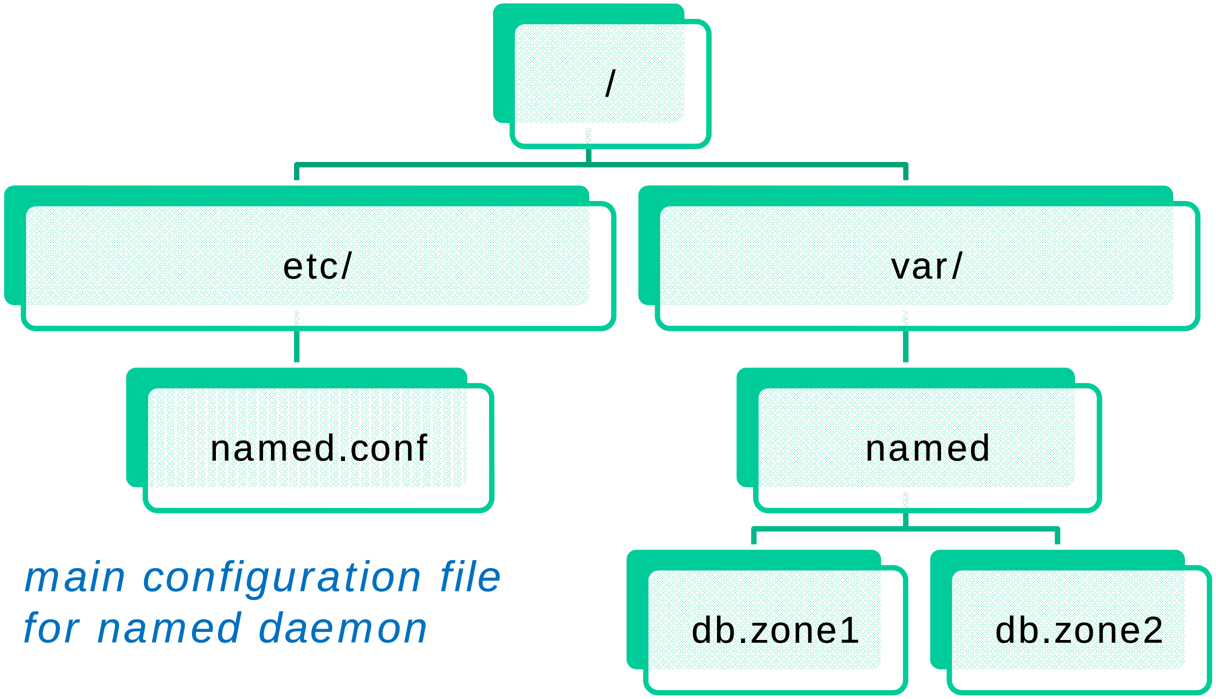
Installing DNS service

```
[root@elrond packages]# ls {bind,caching}*
bind-9.3.6-4.P1.el5_4.2.i386.rpm
bind-libs-9.3.6-4.P1.el5_4.2.i386.rpm
bind-utils-9.3.6-4.P1.el5_4.2.i386.rpm
caching-nameserver-9.3.6-4.P1.el5_4.2.i386.rpm

[root@elrond packages]# rpm -Uvh bind* caching*
Preparing...                ########################################### [100%]
   1:bind-libs              ########################################### [ 25%]
   2:bind                   ########################################### [ 50%]
   3:bind-utils             ########################################### [ 75%]
   4:caching-nameserver     ########################################### [100%]
[root@elrond packages]#
```

Use the rpm command to install the rpm package files

Installing and Configuring DNS service

Step 2 *Customize the configuration files*



main configuration file for named daemon

zone database files for each forward and reverse lookup zone

named.conf

```
[root@elrond packages]# cat /etc/named.conf
options {
        directory "/var/named";
        /*
        * If there is a firewall between you and nameservers you want
        * to talk to, you might need to uncomment the query-source
        * directive below. Previous versions of BIND always asked
        * questions using port 53, but BIND 8.1 uses an unprivileged
        * port by default.
        */
        // query-source address * port 53;
};

//
// a caching only nameserver config
//
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "rivendell" IN {
        type master;
        file "db.rivendell";
        allow-update { none; };
};

zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "db.2.168.192";
        allow-update { none; };
};

// A key file needs to be referenced for use by rndc
include "/etc/rndc.key“;
```

***options** clause – specifies the location of the zone files and can control source port used for queries for firewalls*

***controls** clause – access controls for remote administration services e.g. the rndc utility*

***zone** clauses – specifies zone databases for ., localhost (forward and reverse) and each zone (forward and reverse) this DNS server is responsible for*

***key** clause (included) – specifies a key to use to authenticate various actions or use of the rndc utility*

named.conf

***options** clause – specifies the location of the zone files and can control source port used for queries for firewalls*

```
[root@elrond]# cat /etc/named.conf
options {
        directory "/var/named";
        /*
        * If there is a firewall between you and nameservers you want
        * to talk to, you might need to uncomment the query-source
        * directive below. Previous versions of BIND always asked
        * questions using port 53, but BIND 8.1 uses an unprivileged
        * port by default.
        */
        // query-source address * port 53;
};
< snipped >
```

This is where the zone database files reside

Highlighted text is all comments

named.conf

***controls** clause – access controls for remote administration services e.g. the rndc utility*

```
[root@elrond packages]# cat /etc/named.conf

< snipped >

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

<snipped>
```

IP address on server that will accept connections from the rndc utility

hosts that are allowed access

key to use for authentication

named.conf

```
[root@elrond packages]# cat /etc/named.conf
< snipped >
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "rivendell" IN {
        type master;
        file "db.rivendell";
        allow-update { none; };
};

zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "db.2.168.192";
        allow-update { none; };
};
< snipped >
```

***zone** clauses – specifies zone databases for ., localhost (forward and reverse) and each zone (forward and reverse) this DNS server is responsible for*

In Lab 7 you will setup forward and reverse zones for the Rivendell domain

named.conf

key *clause (included) – specifies a key to use to authenticate various actions or use of the rndc utility*

```
[root@elrond]# cat /etc/named.conf
< snipped >

// A key file needs to be referenced for use by rndc.
include "/etc/rndc.key";



[root@elrond]# cat /etc/rndc.key
key "rndckey" {
        algorithm       hmac-md5;
        secret          "JzQP0lELDl77xshHK96ZeILDiNMtdqwehs8rMpmVHAXYvYb1jQBqr50Snsrp";
};
```

forward
lookup
zone
database

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

TTL = Time to live. How long a DNS record from this zone should be cached.

The longer the TTL value the faster domain resolution time periods will be.

Examples:

$TTL 86400
$TTL 1440m
$TTL 24h
$TTL 1d

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.       IN SOA elrond.rivendell. root.rivendell. (
                 2009040304      ; serial number
                 60              ; refresh rate in seconds
                 15              ; retry in seconds
                 1209600         ; expire in seconds
                 300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.       IN NS elrond.rivendell.
;
;Address Records
localhost        IN A 127.0.0.1
legolas          IN A 192.168.2.105
elrond           IN A 192.168.2.107
galadriel        IN A 192.168.2.108
william          IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Primary domain name

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.       IN SOA elrond.rivendell. root.rivendell. (
                 2009040304      ; serial number
                 60              ; refresh rate in seconds
                 15              ; retry in seconds
                 1209600         ; expire in seconds
                 300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.       IN NS elrond.rivendell.
;
;Address Records
localhost        IN A 127.0.0.1
legolas          IN A 192.168.2.105
elrond           IN A 192.168.2.107
galadriel        IN A 192.168.2.108
william          IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Class of the zone

IN = Internet

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Record type

SOA = Start of Authority

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

The primary DNS server for this zone

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

The email address of the person/authority in charge. Note the "@" is replaced by a "."

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Serial number, typically YYYYMMDDNN.

***Must be updated** to a larger number whenever zone file is updated or the changes will be ignored by BIND*

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Refresh rate

How often the secondary server should poll the primary to refresh it data

It is set to only 60 seconds for Lab 7 so we can see zone transfers happen quickly.

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Retry

A value typically an hour or less that the secondary server should repeat an update request if the primary failed to respond.

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Expire

In the case where the secondary server can no longer reach the primary, this is the amount of time the zone information can be used.

secondarys servers will stop responding to requests for this zone once the data has expired.

A successful refresh (a zone update) will reset the timers and the cycle will begin again.

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Minimum

How long a non-authoritative server should cache an entry in case of failed lookups

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

NS (Name Server) records indicate the authoritative name servers for this zone.

Public domains are required to have at least two name servers.

Private domains may have just one.

Zone file

```
[root@elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009040304      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.
;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
galadriel       IN A 192.168.2.108
william         IN A 192.168.2.114
;
;CNAME records
[root@elrond ~]#
```

Each A records matches a hostname with an IPv4 address.

reverse lookup zone database

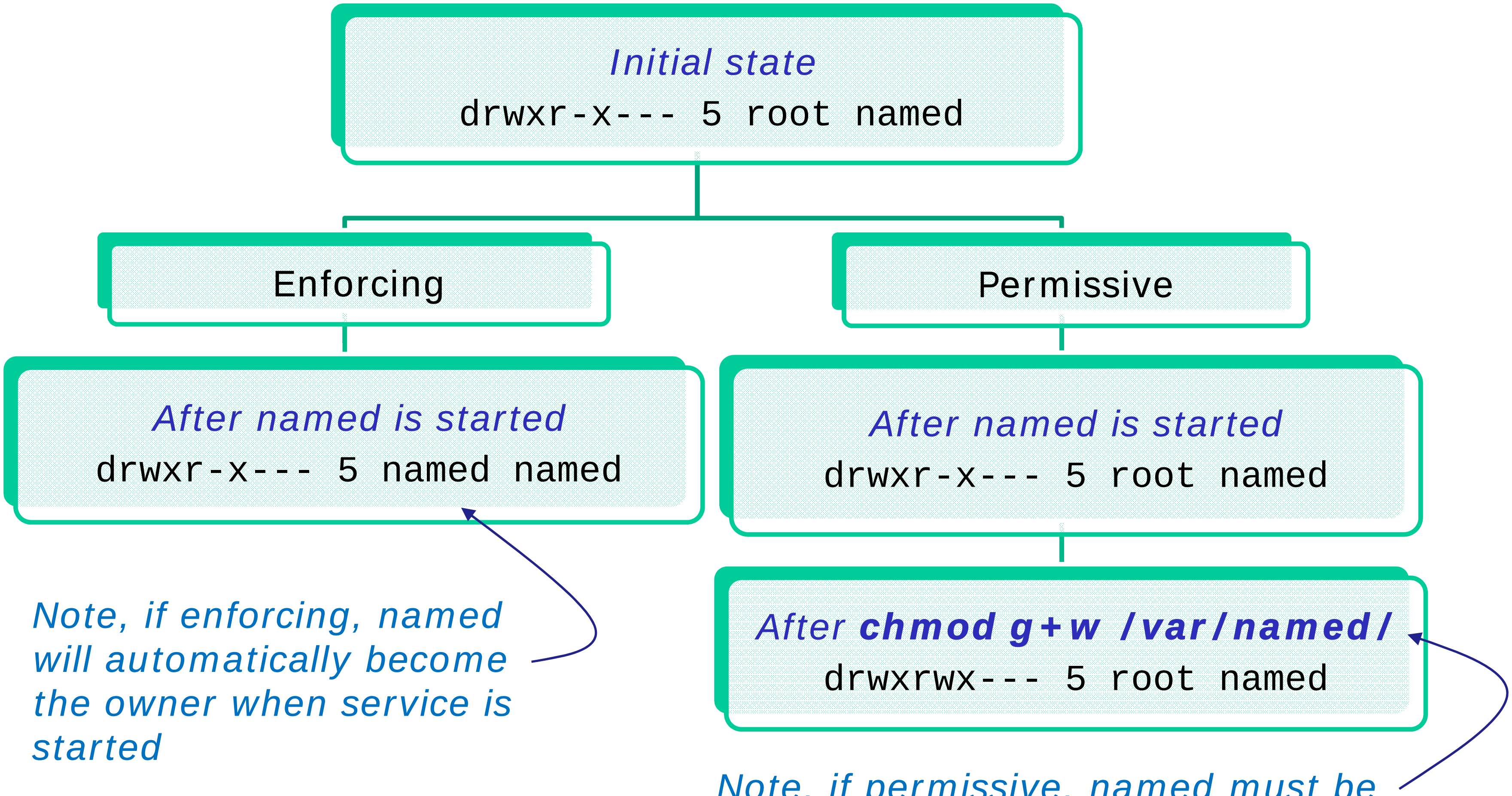
Zone file

```
[root@elrond named]# cat db.2.168.192
$TTL    86400
;192.168.2.* Reverse Zone Definition
;
2.168.192.in-addr.arpa. IN SOA  elrond.rivendell. root.rivendell.  (
                                      2009040311 ; Serial
                                      60         ; Refresh
                                      15         ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
;
;Name Server Records
;
2.168.192.in-addr.arpa. IN NS elrond.rivendell.
;
;Address Records
105                     IN PTR  legolas.rivendell.
107                     IN PTR  elrond.rivendell.
108                     IN PTR  galadriel.rivendell.
114                     IN PTR  william.rivendell.
[root@elrond named]#
```

Note the use of PTR records to match the final portion of the IP address to a host name

Secondary Nameserver must allow named to write to /var/named/

Step 2 ***/var/named*** *directory permissions and ownership*



Initial state

```
drwxr-x--- 5 root named
```

Enforcing

After named is started

```
drwxr-x--- 5 named named
```

Permissive

After named is started

```
drwxr-x--- 5 root named
```

After ***chmod g+w /var/named/***

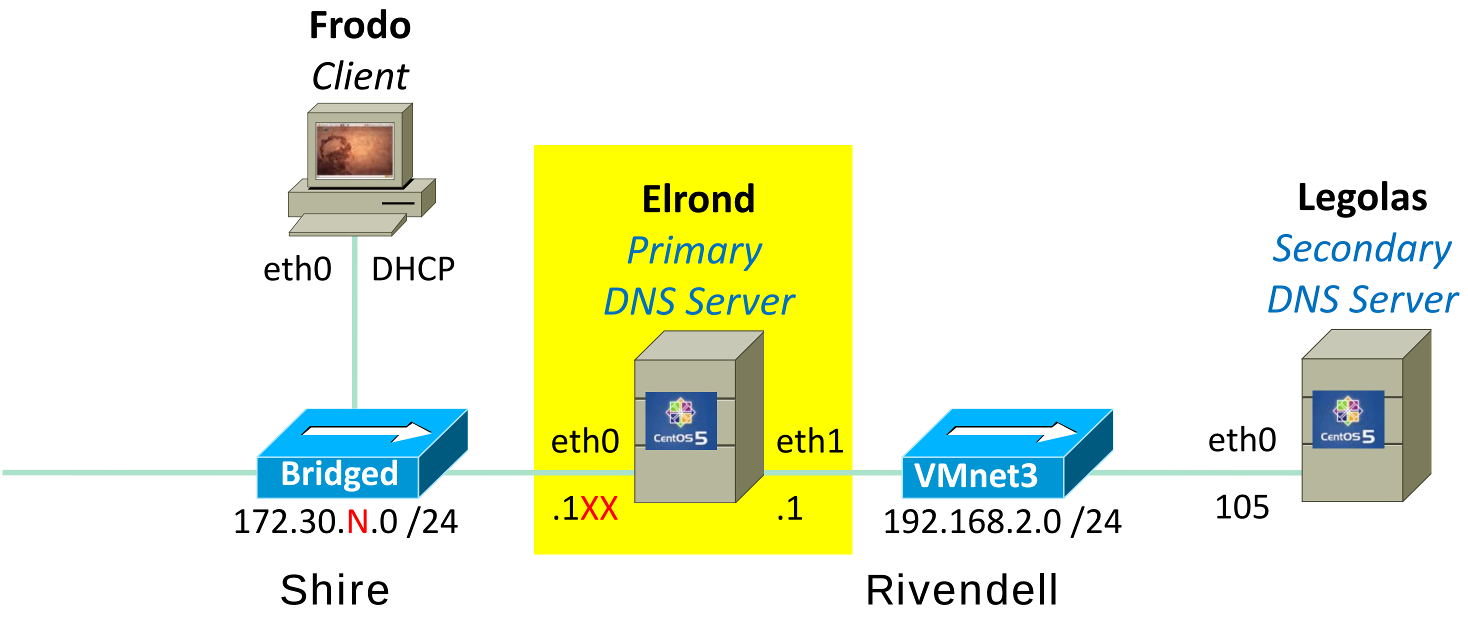
```
drwxrwx--- 5 root named
```

Note, if enforcing, named will automatically become the owner when service is started

Note, if permissive, named must be manually made the owner

Installing and Configuring DNS Service (Red Hat Family)

Step 3 *Firewall modifications*



Elrond is the primary nameserver

Open UDP 53 to allow incoming DNS requests

Open TCP port 53 to allow zone transfers to secondary servers

Allow forwarding of DNS queries to Internet DNS servers

Installing and Configuring DNS Service

CentOS default firewall on primary nameserver

```
[root@elrond etc]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
6    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
7    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
8    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
9    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
10   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@elrond etc]#
```

Forward traffic is being subjected to input rules which will block forwarded DNS requests to Internet servers

UDP/TCP port 53 is not open by default which will block incoming DNS requests and zone transfer file requests

Installing and Configuring DNS Service

CentOS firewall modifications on primary nameserver

Open UDP port 53 for DNS queries

```
iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 53 -j ACCEPT
```

Open TCP port 53 for zone transfers

```
iptables -I RH-Firewall-1-INPUT 6 -s 192.168.2.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
```

Allow unrestricted traffic forwarding

```
iptables -D FORWARD 1
```

Provide NAT service so Rivendell hosts have Internet access

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

The last rule enables the secondary DNS server on Legolas to send DNS queries to other Internet DNS servers

Installing and Configuring DNS Service

CentOS modified firewall for primary nameserver

```
[root@elrond bin]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (1 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     tcp  --  192.168.2.0/24       0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@elrond bin]#
```

Forwarded traffic is no longer blocked

UDP port 53 and TCP port 53 are now open to allow DNS queries and zone transfer file requests

Installing and Configuring DNS Service

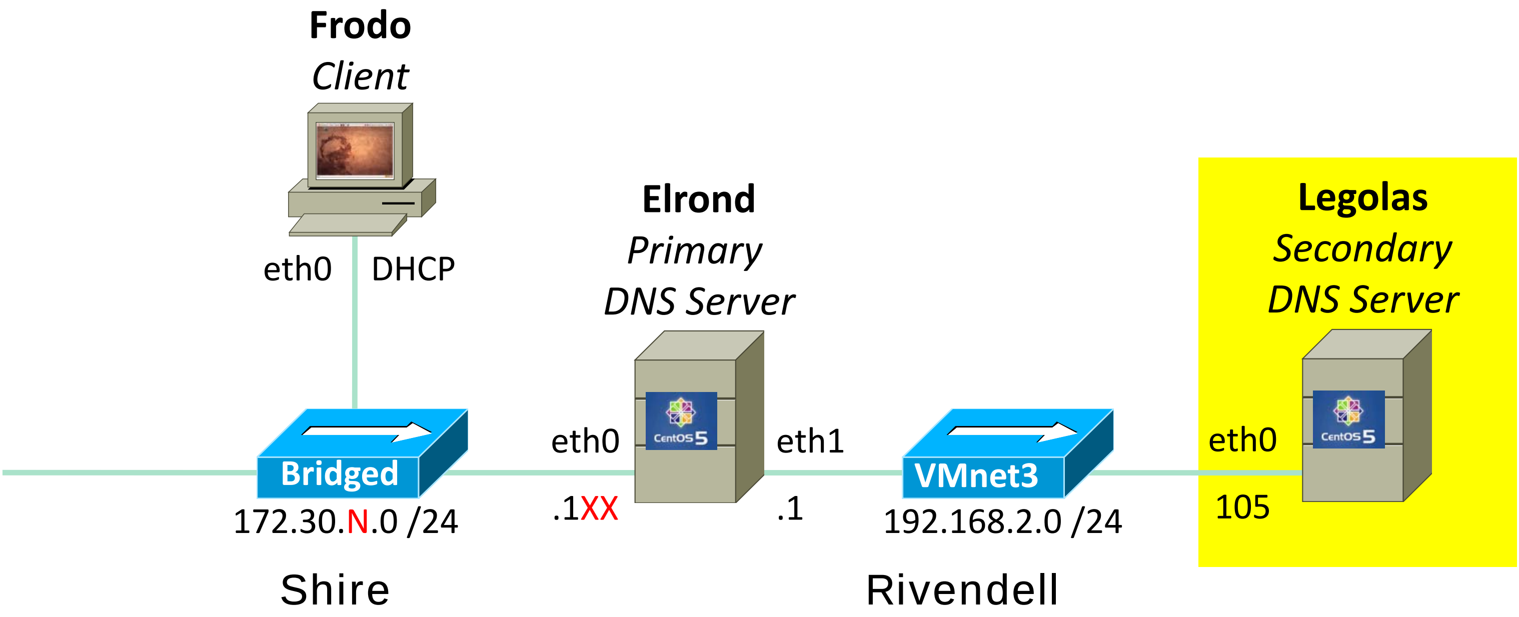
CentOS modified firewall for primary nameserver

```
[root@elrond bin]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@elrond bin]#
```

Provide NAT service so Rivendell hosts have Internet access. Note: This allows the secondary name server on Legolas to make DNS queries to other Internet name servers.

Installing and Configuring DNS Service (Red Hat Family)

Step 3 *Firewall modifications*



Legolas is the secondary nameserver

Open UDP 53 to allow incoming DNS requests

Installing and Configuring DNS Service

CentOS default firewall on secondary nameserver

```
[root@legolas etc]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
6    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
7    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
8    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
9    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
10   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@elrond etc]#
```

UDP port 53 is not open by default which will block incoming DNS requests

Installing and Configuring DNS Service

CentOS firewall modifications on secondary nameserver

Open UDP port 53 for DNS queries

```
iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 53 -j ACCEPT
```

Installing and Configuring DNS Service

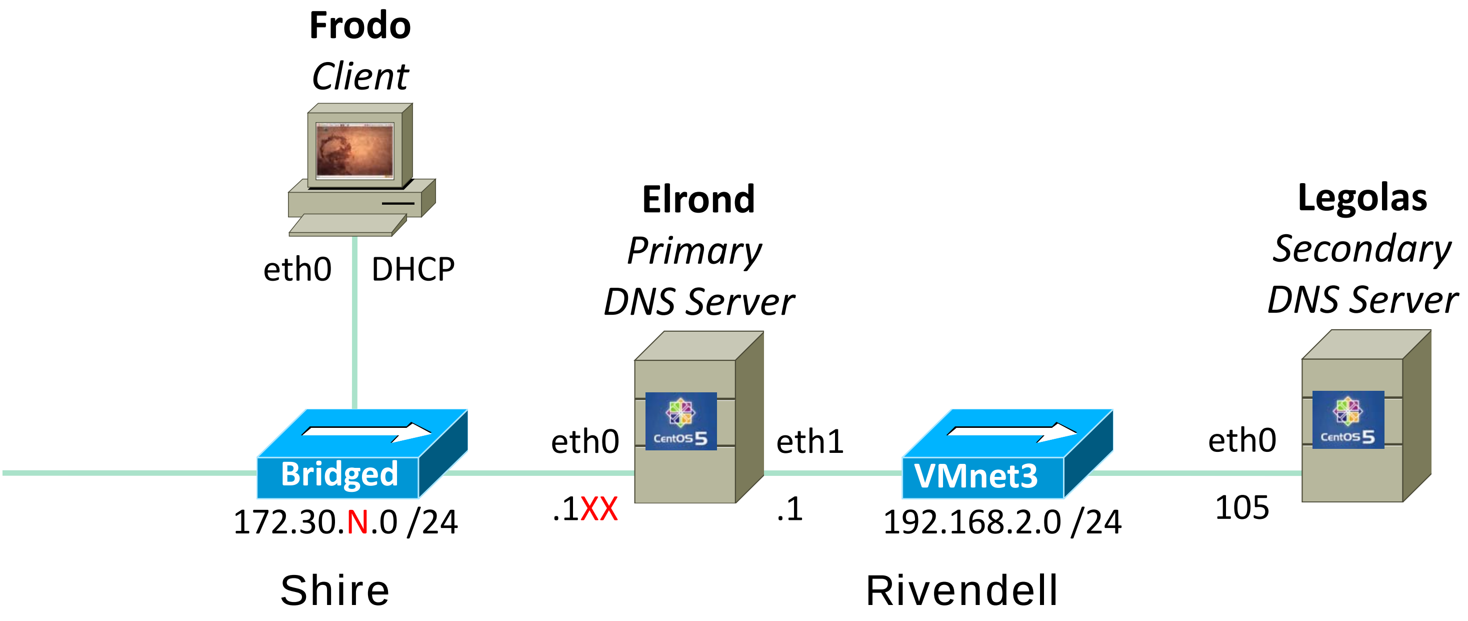
CentOS modified firewall for secondary nameserver

```
[root@legolas bin]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
6    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
7    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
8    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
9    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
10   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
11   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@legolas bin]#
```

UDP port 53 is now open to allow DNS requests

Installing and Configuring DNS Service (Red Hat Family)

Step 3 *SELinux modifications (used in Lab 7)*



Installing and Configuring DNS service

Step 4 *SELinux*

- On the primary and secondary server leave the SELinux setting as Enforcing
- On the secondary server, make the following change to allow the named daemon (named) to write zone files in /var/named/

```
setsebool -P named_write_master_zones=1
```

https://bugzilla.redhat.com/show_bug.cgi?id=545128
https://bugzilla.redhat.com/show_bug.cgi?id=147824

SELinux Administration (sidetrack)

Set permissive mode

```
[root@legolas ~]# setenforce permissive
[root@legolas ~]# getenforce
Permissive
```

Set enforcing mode

```
[root@legolas ~]# setenforce enforcing
[root@legolas ~]# getenforce
Enforcing
```

Show SELinux status

```
[root@legolas ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

SELinux Administration (sidetrack)

Set SELinux boolian flag on

```
[root@legolas ~]# setsebool –P named_write_master_zones=1
```

Show SELinux boolian flag

```
[root@legolas ~]# getsebool named_write_master_zones
named_write_master_zones --> on
```

Set SELinux boolian flag off

```
[root@legolas ~]# setsebool –P named_write_master_zones=0
```

Show SELinux boolian flag

```
[root@legolas ~]# getsebool named_write_master_zones
named_write_master_zones --> off
```

Note, the –P option on setsebool makes the setting persistent across system restarts

SELinux Administration (sidetrack)

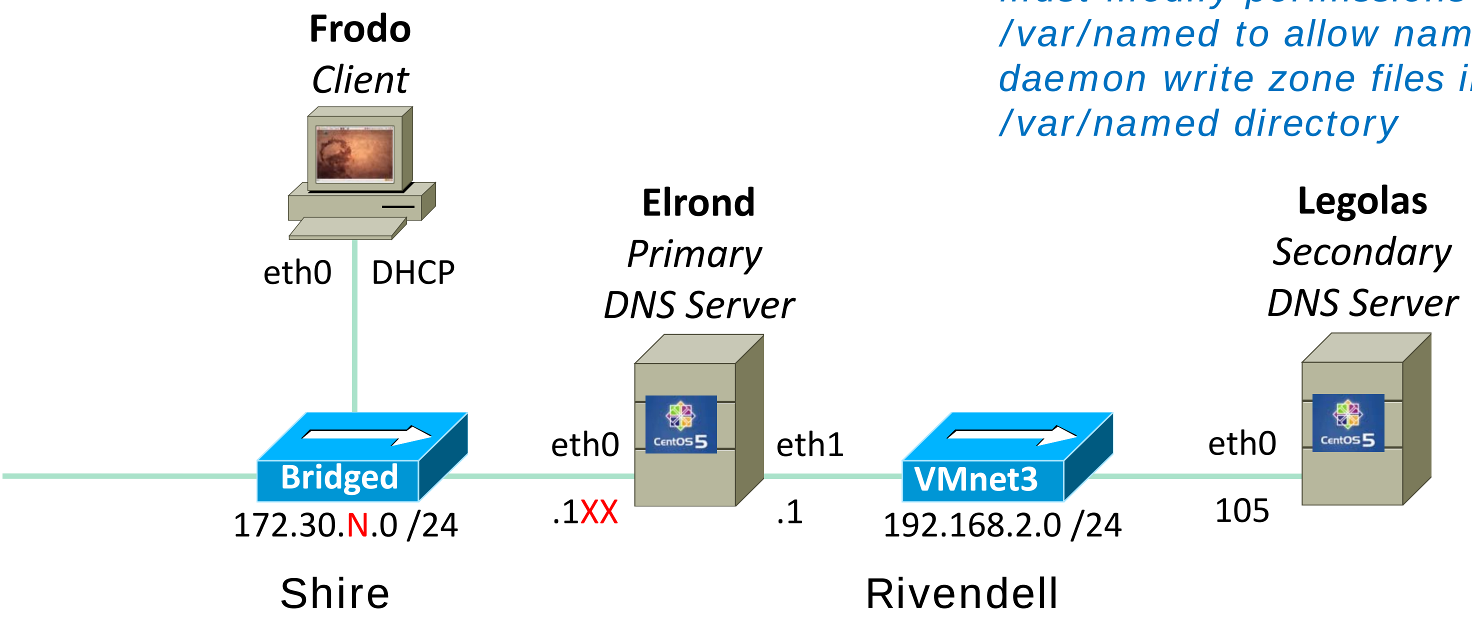
Show all SELinux boolean flags

```
[root@legolas ~]# getsebool –a
NetworkManager_disable_trans --> off
allow_console_login --> off
allow_cvs_read_shadow --> off
allow_daemons_dump_core --> on
allow_daemons_use_tty --> on
allow_domain_fd_use --> on
allow_execheap --> off
allow_execmem --> on
allow_execmod --> off
allow_execstack --> on
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
< snipped >
```

Installing and Configuring DNS Service (Red Hat Family)

Step 3 *SELinux modifications*

*Note, if you do run the **secondary** nameserver in **Permissive** mode, then you must modify permissions on /var/named to allow named daemon write zone files into the /var/named directory*



*Note, if you run the **secondary** nameserver in **Enforcing** mode, then you must use the setsebool command to allow the named daemon to write zone files to /var/named/*

Installing and Configuring DNS service

Step 4 *SELinux*

Elrond (permissive)

- no sebool commands needed
- no owner changes needed for /var/named
- no permission changes needed for /var/named

Primary

Legolas (permissive)

- no sebool commands needed
- no owner changes needed for /var/named
- permission change required (for named to write zone files)

```
[root@legolas ~]# ls -ld /var/named
drwxr-x--- 5 root named 4096 Apr 14 08:48 /var/named

[root@legolas ~]# chmod g+w /var/named/
[root@legolas ~]# ls -ld /var/named
drwxrwx--- 5 root named 4096 Apr 14 08:48 /var/named
```

Secondary

*Note, if you do run the **secondary** nameserver in **Permissive** mode, then you must modify permissions on /var/named to allow named daemon write zone files into the /var/named directory*

Installing and Configuring DNS service

Step 4 *SELinux*

Elrond (enforcing)

- no sebool commands
- no owner changes
- no permission changes

Primary

Legolas (enforcing)

- **setsebool -P named_write_master_zones=1**
- no owner changes needed for /var/named
- no permission changes needed for /var/named

Secondary

Note, named was automatically made owner of this directory

```
[root@legolas bin]# ls -ld /var/named
drwxr-x--- 5 named named 4096 Apr 14 10:16 /var/named
```

*Note, if you run the **secondary** nameserver in **Enforcing** mode, then you must use the setsebool command above to allow the named daemon to write zone files to /var/named/*

On the Secondary Nameserver

Step 4 *SELinux and Permissions*

	Elrond commands	Legolas commands
Enforcing	NA	setsebool -P named_write_master_zones=1
Permissive	NA	chmod g+w /var/named/

No changes need to be made on the primary nameserver

On the secondary nameserver, named needs to be able to write zone files to the /var/named directory

Installing and Configuring DNS service

Step 5 *Start service*

```
[root@arwen ~]# service named start
Starting named:                                                [  OK  ]
```

Installing and Configuring DNS service

If service is already running use the following to reread configuration files:

```
service named restart
```

or

```
rndc reload
```

Installing and Configuring DNS service

Step 6 Configure automatic service startup

To automatically start service at system boot use:

```
[root@elrond ~]# chkconfig named on
[root@elrond ~]# chkconfig --list named
named           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

To not start service at system boot use:

```
[root@elrond ~]# chkconfig named off
[root@elrond ~]# chkconfig --list named
named           0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

Installing and Configuring DNS service

Step 7 *Monitor and verify service is running*

named process

```
[root@elrond bin]# ps -ef | grep named
named     9869     1  0 14:31 ?        00:00:00 /usr/sbin/named -u named
root      9984  3200  0 14:48 pts/0    00:00:00 grep named
[root@elrond bin]#
```

Installing and Configuring DNS service

Step 7 *Monitor and verify service is running*

```
[root@elrond bin]# service named status
number of zones: 4
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/1000
tcp clients: 0/100
server is up and running
named (pid  9869) is running...
[root@elrond bin]#
```

Installing and Configuring DNS service

Step 7 *Verify service is running*

netstat

```
[root@elrond bin]# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:876                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 192.168.2.1:53              0.0.0.0:*                   LISTEN
tcp        0      0 172.30.1.125:53             0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:53                0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:953               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
[root@elrond bin]#
```

*Use **netstat –tl** command to see what port names your system is listening for requests on*

Installing and Configuring DNS service

Step 7 *Verify service is running*

netstat

```
[root@elrond bin]# netstat -uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 192.168.2.1:53              0.0.0.0:*
udp        0      0 172.30.1.125:53             0.0.0.0:*
udp        0      0 127.0.0.1:53                0.0.0.0:*
udp        0      0 0.0.0.0:870                 0.0.0.0:*
udp        0      0 0.0.0.0:5353                0.0.0.0:*
udp        0      0 0.0.0.0:873                 0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 0.0.0.0:33530               0.0.0.0:*
udp        0      0 :::36992                    :::*
udp        0      0 :::5353                     :::*
[root@elrond bin]#
```

*Use **netstat -tln** command to see what port numbers your system is listening for requests on*

Installing and Configuring DNS service

Try it!

```
[root@elrond bin]# host elrond
elrond.rivendell has address 192.168.2.1

[root@elrond bin]# host legolas
legolas.rivendell has address 192.168.2.105

[root@elrond bin]# host 192.168.2.105
105.2.168.192.in-addr.arpa domain name pointer legolas.rivendell.
```

Installing and Configuring DNS service

Step 8 *Troubleshooting*

Problem: primary to secondary transfer failing

From /var/log/messages:

```
Apr 13 10:22:43 legolas named[13585]: the working directory is not writable
Apr 13 10:22:43 legolas named[13585]: zone 0.0.127.in-addr.arpa/IN: loaded serial
1997022700
Apr 13 10:22:43 legolas named[13585]: zone localhost/IN: loaded serial 42
Apr 13 10:22:43 legolas named[13585]: running
Apr 13 10:22:43 legolas named[13585]: zone rivendell/IN: Transfer started.
Apr 13 10:22:43 legolas named[13585]: transfer of 'rivendell/IN' from
192.168.2.1#53: connected using 192.168.2.105#50197
Apr 13 10:22:43 legolas named[13585]: dumping master file: tmp-gU4SMMpaFs: open:
permission denied
Apr 13 10:22:43 legolas named[13585]: transfer of 'rivendell/IN' from
192.168.2.1#53: failed while receiving responses: permission denied
```

Solution:

Configure SElinux to allow named to write zone files on secondary:

1. Run **lokkit** on secondary and change SELinux setting from Enforcing to Permissive
2. or **setsebool -P named_write_master_zones=1**
   (https://bugzilla.redhat.com/show_bug.cgi?id=545128)

Installing and Configuring DNS service

Step 8 *Troubleshooting*

Problem: primary to secondary transfer failing

From /var/log/messages:

```
Apr  6 07:01:15 legolas named[16429]: zone rivendell/IN: refresh:
retry limit for master 192.168.2.107#53 exceeded (source 0.0.0.0#0)
Apr  6 07:01:15 legolas named[16429]: zone rivendell/IN: Transfer
started.
Apr  6 07:01:15 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: failed to connect: host unreachable
Apr  6 07:01:15 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: end of transfer
```

Solution:

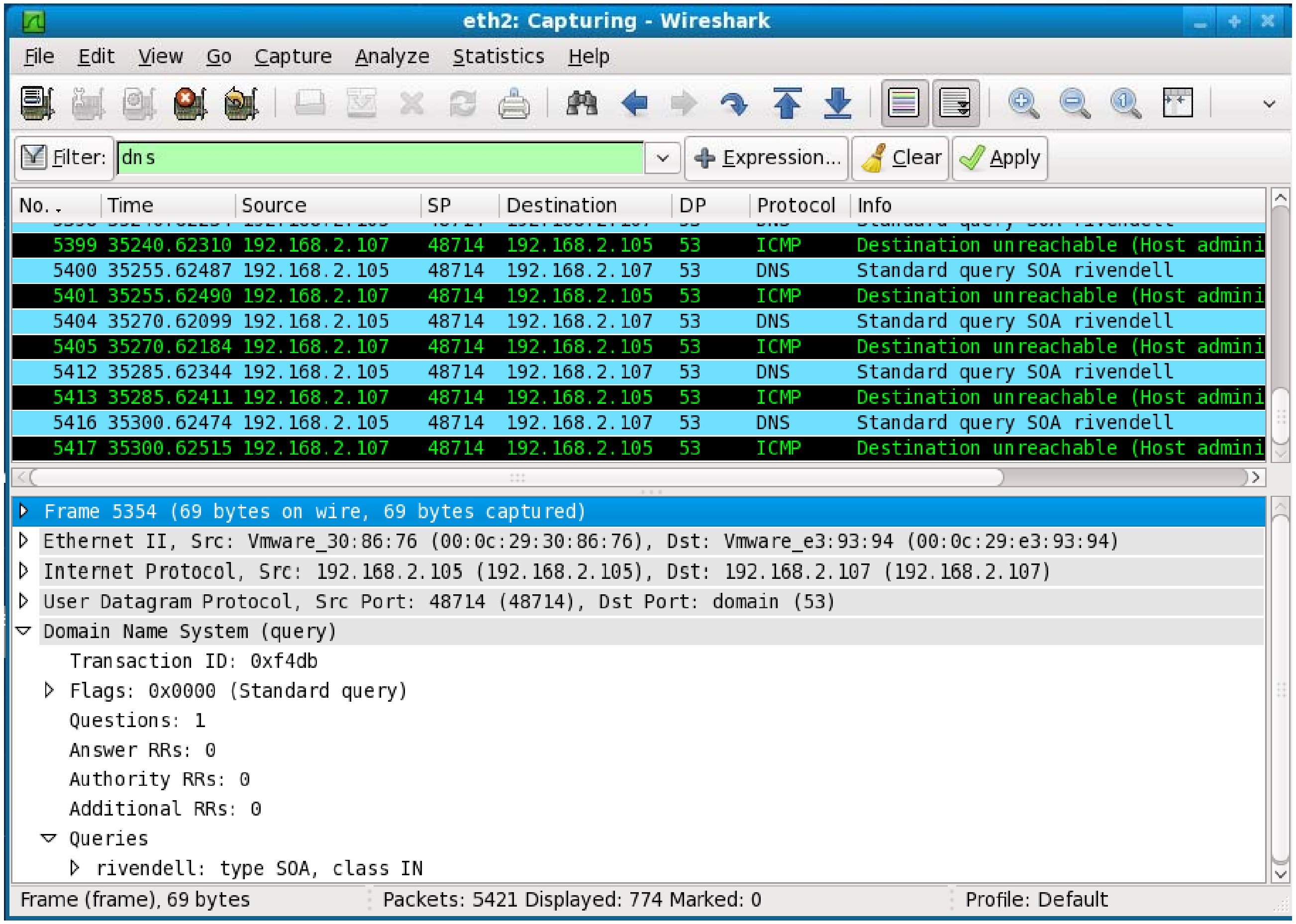
Firewall on master is blocking connection by secondary for transfer

1. Open UDP port 53 (for DNS requests) and TCP port 53 (for zone file transfers) on primary

Installing and Configuring DNS service

Step 8 *Troubleshooting*

Zone transfer failing when blocked by firewall on primary


eth2: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: dns
Expression... Clear Apply

```
No. .  Time         Source          SP     Destination     DP   Protocol  Info
 5399 35240.62310 192.168.2.107   48714  192.168.2.105   53   ICMP      Destination unreachable (Host admini
 5400 35255.62487 192.168.2.105   48714  192.168.2.107   53   DNS       Standard query SOA rivendell
 5401 35255.62490 192.168.2.107   48714  192.168.2.105   53   ICMP      Destination unreachable (Host admini
 5404 35270.62099 192.168.2.105   48714  192.168.2.107   53   DNS       Standard query SOA rivendell
 5405 35270.62184 192.168.2.107   48714  192.168.2.105   53   ICMP      Destination unreachable (Host admini
 5412 35285.62344 192.168.2.105   48714  192.168.2.107   53   DNS       Standard query SOA rivendell
 5413 35285.62411 192.168.2.107   48714  192.168.2.105   53   ICMP      Destination unreachable (Host admini
 5416 35300.62474 192.168.2.105   48714  192.168.2.107   53   DNS       Standard query SOA rivendell
 5417 35300.62515 192.168.2.107   48714  192.168.2.105   53   ICMP      Destination unreachable (Host admini
```

```
▷ Frame 5354 (69 bytes on wire, 69 bytes captured)
▷ Ethernet II, Src: Vmware_30:86:76 (00:0c:29:30:86:76), Dst: Vmware_e3:93:94 (00:0c:29:e3:93:94)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.107 (192.168.2.107)
▷ User Datagram Protocol, Src Port: 48714 (48714), Dst Port: domain (53)
▽ Domain Name System (query)
    Transaction ID: 0xf4db
  ▷ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▷ rivendell: type SOA, class IN
```

Frame (frame), 69 bytes   Packets: 5421 Displayed: 774 Marked: 0   Profile: Default

Installing and Configuring DNS service

Step 9 *Monitor log files*

```
[root@elrond ~]# cat /var/log/messages | grep telnet
Apr 14 15:05:24 elrond named[10126]: using default UDP/IPv4 port range: [1024, 65535]
Apr 14 15:05:24 elrond named[10126]: using default UDP/IPv6 port range: [1024, 65535]
Apr 14 15:05:24 elrond named[10126]: listening on IPv4 interface lo, 127.0.0.1#53
Apr 14 15:05:24 elrond named[10126]: listening on IPv4 interface eth0, 172.30.1.125#53
Apr 14 15:05:24 elrond named[10126]: listening on IPv4 interface eth1, 192.168.2.1#53
Apr 14 15:05:24 elrond named[10126]: command channel listening on 127.0.0.1#953
Apr 14 15:05:24 elrond named[10126]: the working directory is not writable
Apr 14 15:05:24 elrond named[10126]: zone 0.0.127.in-addr.arpa/IN: loaded serial
1997022700
Apr 14 15:05:24 elrond named[10126]: zone 2.168.192.in-addr.arpa/IN: loaded serial
2010041500
Apr 14 15:05:24 elrond named[10126]: zone localhost/IN: loaded serial 42
Apr 14 15:05:24 elrond named[10126]: zone rivendell/IN: loaded serial 2010041500
Apr 14 15:05:24 elrond named[10126]: running
Apr 14 15:05:24 elrond named[10126]: zone 2.168.192.in-addr.arpa/IN: sending notifies
(serial 2010041500)
Apr 14 15:05:24 elrond named[10126]: client 192.168.2.1#11553: received notify for zone
'2.168.192.in-addr.arpa'
[root@elrond bin]#
```

*Use **tail –f /var/log/messages** to monitor in real time*

Installing and Configuring DNS service

Step 10 *Configure additional security*

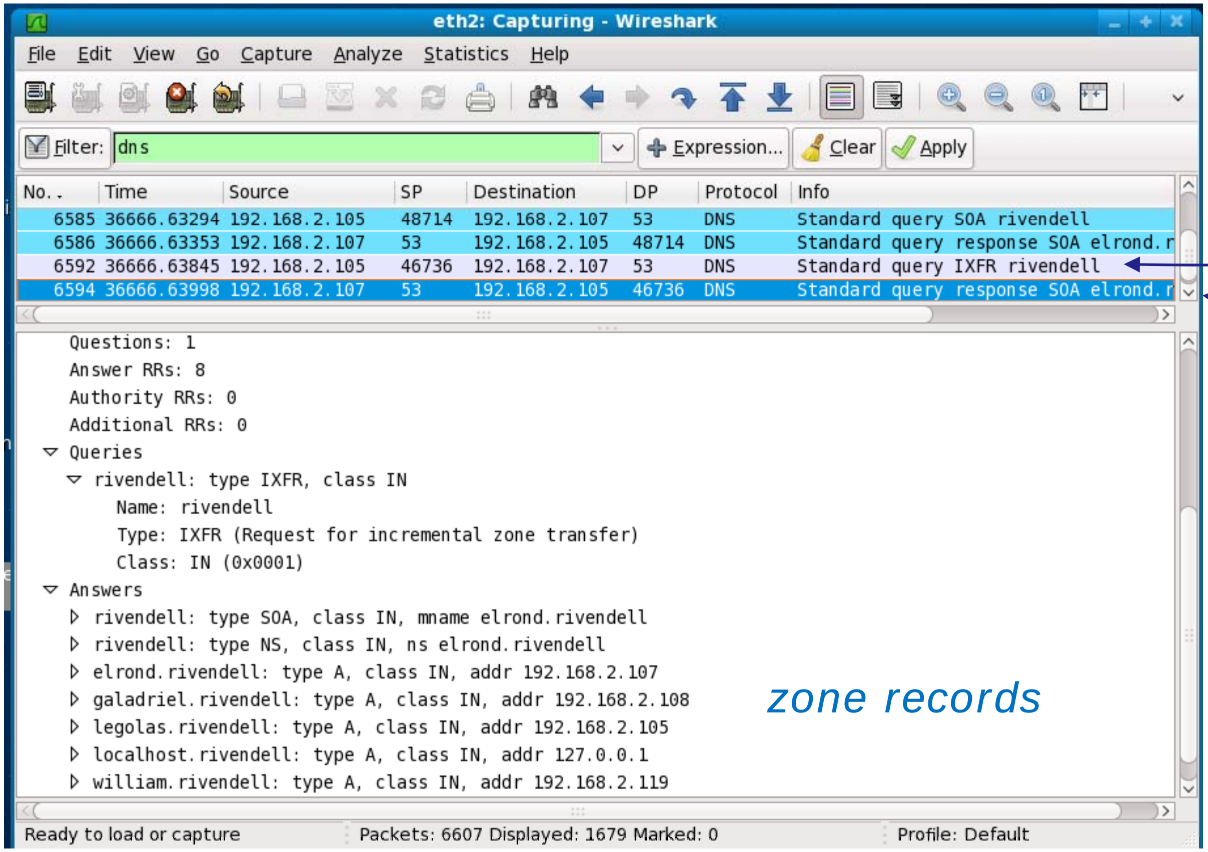
See 15.15 in the text book for more information

zone transfer

Zone transfer

The secondary server does this to obtain the zone databases from the primary server

A **successful** zone transfer


eth2: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: dns
Expression...
Clear
Apply

```
No..  Time         Source         SP     Destination    DP     Protocol  Info
6585 36666.63294 192.168.2.105  48714  192.168.2.107  53     DNS   Standard query SOA rivendell
6586 36666.63353 192.168.2.107  53     192.168.2.105  48714  DNS   Standard query response SOA elrond.r
6592 36666.63845 192.168.2.105  46736  192.168.2.107  53     DNS   Standard query IXFR rivendell
6594 36666.63998 192.168.2.107  53     192.168.2.105  46736  DNS   Standard query response SOA elrond.r
```

```
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ rivendell: type IXFR, class IN
        Name: rivendell
        Type: IXFR (Request for incremental zone transfer)
        Class: IN (0x0001)
  ▽ Answers
    ▷ rivendell: type SOA, class IN, mname elrond.rivendell
    ▷ rivendell: type NS, class IN, ns elrond.rivendell
    ▷ elrond.rivendell: type A, class IN, addr 192.168.2.107
    ▷ galadriel.rivendell: type A, class IN, addr 192.168.2.108
    ▷ legolas.rivendell: type A, class IN, addr 192.168.2.105
    ▷ localhost.rivendell: type A, class IN, addr 127.0.0.1
    ▷ william.rivendell: type A, class IN, addr 192.168.2.119
```

```
Ready to load or capture    Packets: 6607 Displayed: 1679 Marked: 0    Profile: Default
```

Request from secondary

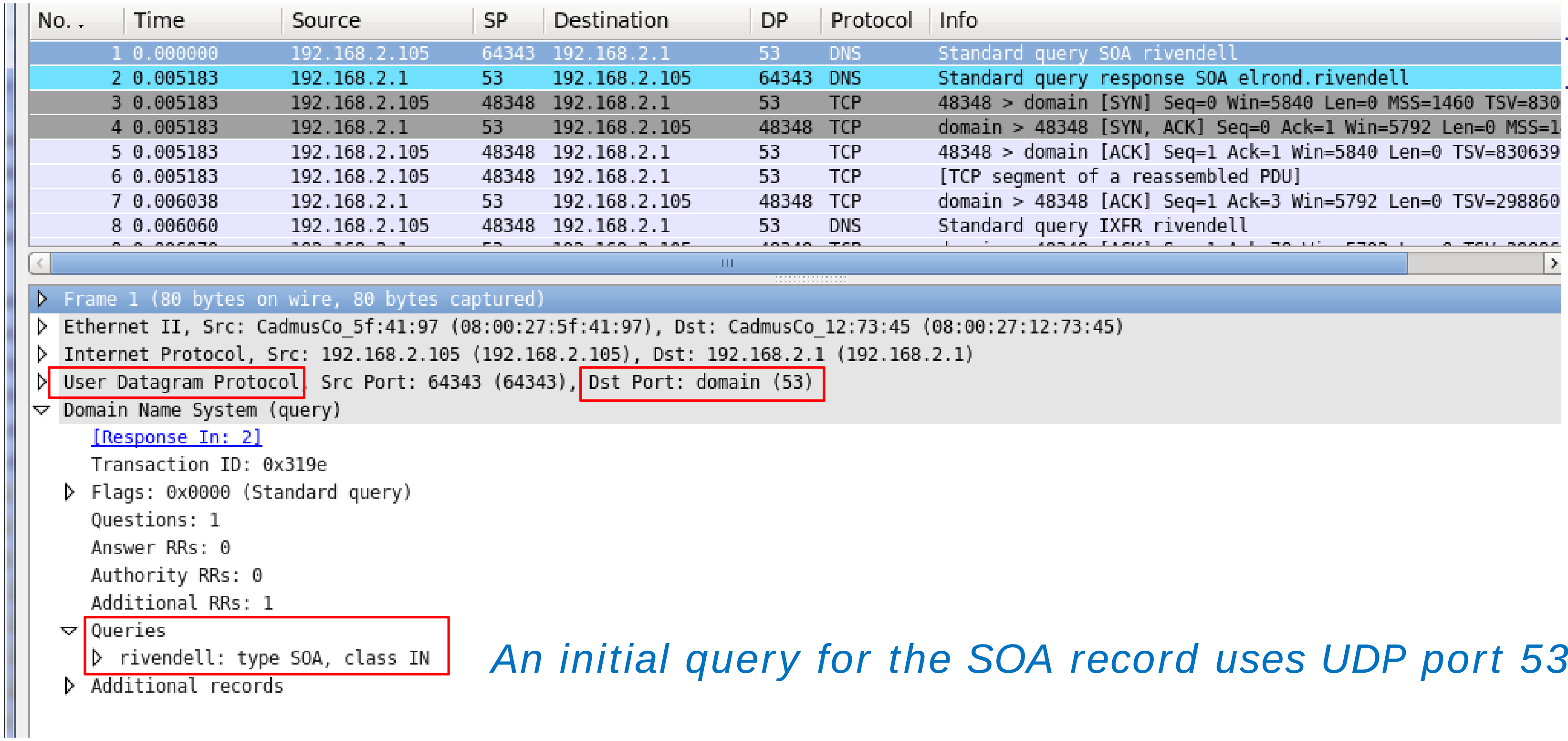
Response from primary

zone records

/var/log/messages:

```
Apr  6 07:30:59 legolas named[16429]: zone rivendell/IN: Transfer started.
Apr  6 07:30:59 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: connected using 192.168.2.105#46736
Apr  6 07:30:59 legolas named[16429]: zone rivendell/IN: transferred serial
2009040309
Apr  6 07:30:59 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: end of transfer
```

Zone transfer involves UPD and TCP requests to port 53



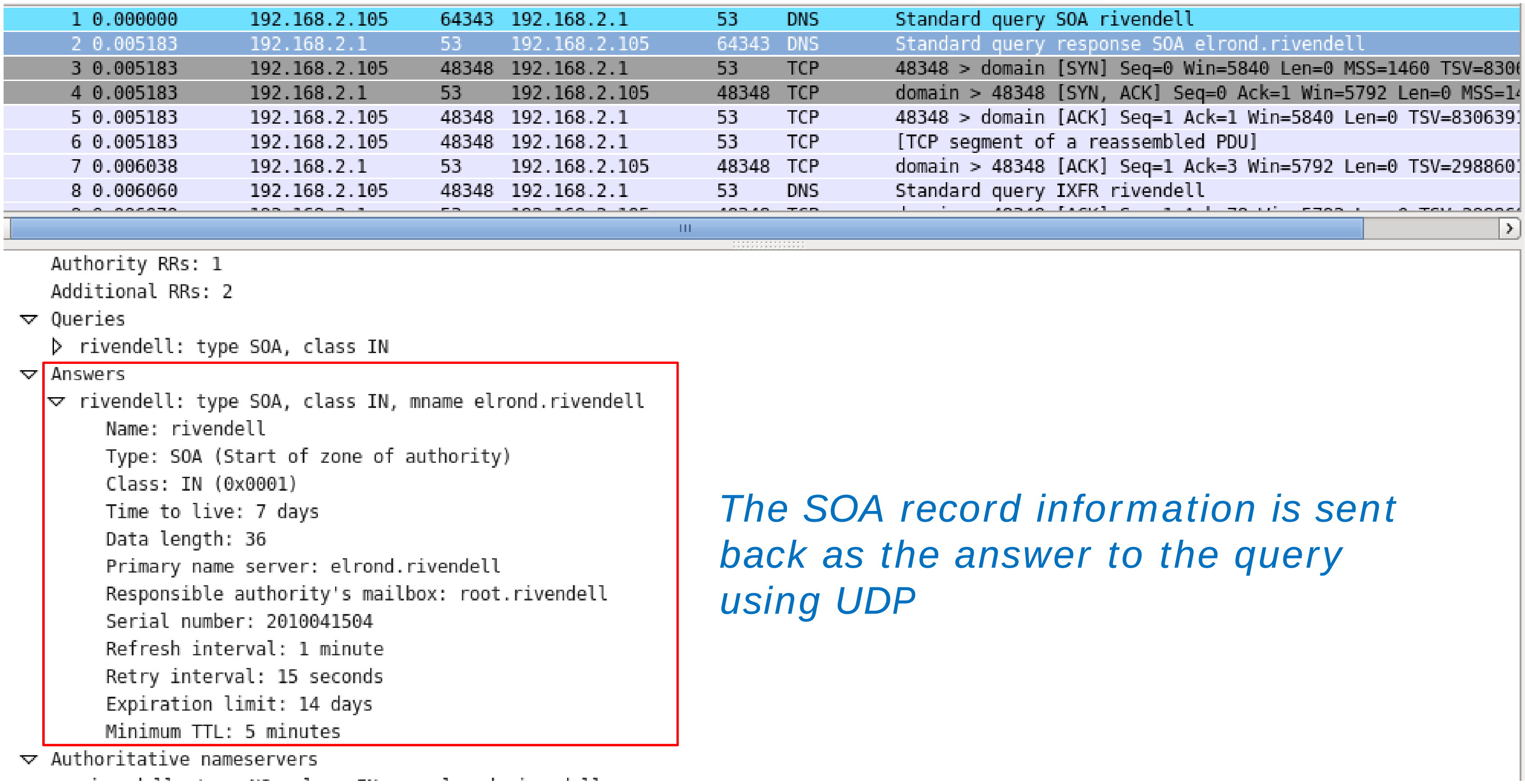
No.	Time	Source	SP	Destination	DP	Protocol	Info
1	0.000000	192.168.2.105	64343	192.168.2.1	53	DNS	Standard query SOA rivendell
2	0.005183	192.168.2.1	53	192.168.2.105	64343	DNS	Standard query response SOA elrond.rivendell
3	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=830
4	0.005183	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
5	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=830639
6	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	[TCP segment of a reassembled PDU]
7	0.006038	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [ACK] Seq=1 Ack=3 Win=5792 Len=0 TSV=298860
8	0.006060	192.168.2.105	48348	192.168.2.1	53	DNS	Standard query IXFR rivendell

```
▷ Frame 1 (80 bytes on wire, 80 bytes captured)
▷ Ethernet II, Src: CadmusCo_5f:41:97 (08:00:27:5f:41:97), Dst: CadmusCo_12:73:45 (08:00:27:12:73:45)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.1 (192.168.2.1)
▷ User Datagram Protocol, Src Port: 64343 (64343), Dst Port: domain (53)
▽ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x319e
  ▷ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▽ Queries
    ▷ rivendell: type SOA, class IN
  ▷ Additional records
```

UDP

An initial query for the SOA record uses UDP port 53

Zone transfer involves UPD and TCP requests to port 53



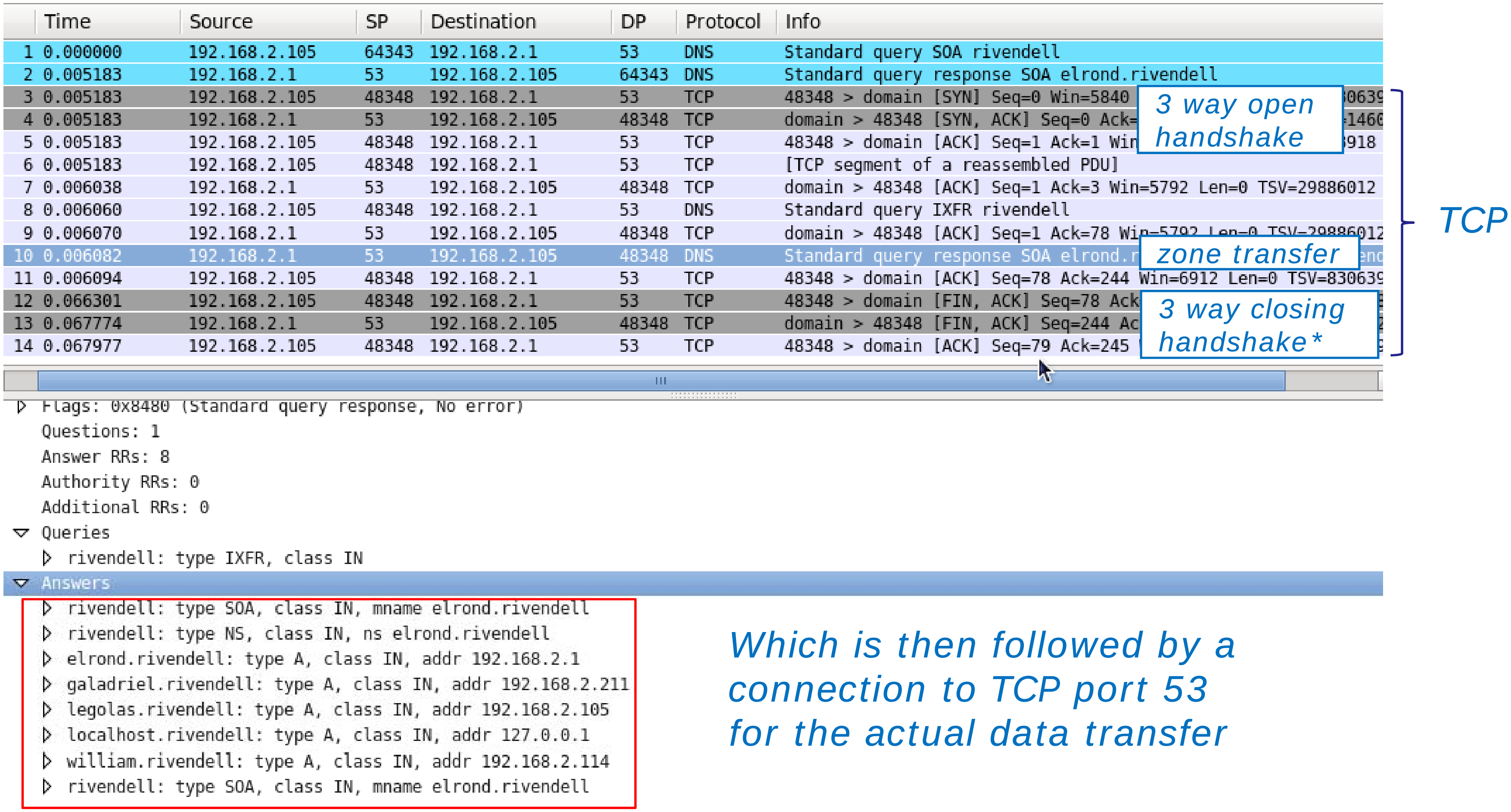
```
  1 0.000000    192.168.2.105   64343  192.168.2.1    53     DNS    Standard query SOA rivendell
  2 0.005183    192.168.2.1     53     192.168.2.105  64343  DNS    Standard query response SOA elrond.rivendell
  3 0.005183    192.168.2.105   48348  192.168.2.1    53     TCP    48348 > domain [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=830
  4 0.005183    192.168.2.1     53     192.168.2.105  48348  TCP    domain > 48348 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
  5 0.005183    192.168.2.105   48348  192.168.2.1    53     TCP    48348 > domain [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=830639
  6 0.005183    192.168.2.105   48348  192.168.2.1    53     TCP    [TCP segment of a reassembled PDU]
  7 0.006038    192.168.2.1     53     192.168.2.105  48348  TCP    domain > 48348 [ACK] Seq=1 Ack=3 Win=5792 Len=0 TSV=298860
  8 0.006060    192.168.2.105   48348  192.168.2.1    53     DNS    Standard query IXFR rivendell
```

```
    Authority RRs: 1
    Additional RRs: 2
  ▽ Queries
    ▷ rivendell: type SOA, class IN
  ▽ Answers
    ▽ rivendell: type SOA, class IN, mname elrond.rivendell
        Name: rivendell
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
        Time to live: 7 days
        Data length: 36
        Primary name server: elrond.rivendell
        Responsible authority's mailbox: root.rivendell
        Serial number: 2010041504
        Refresh interval: 1 minute
        Retry interval: 15 seconds
        Expiration limit: 14 days
        Minimum TTL: 5 minutes
  ▽ Authoritative nameservers
```

} *UDP*

The SOA record information is sent back as the answer to the query using UDP

Zone transfer involves UPD and TCP requests to port 53



	Time	Source	SP	Destination	DP	Protocol	Info
1	0.000000	192.168.2.105	64343	192.168.2.1	53	DNS	Standard query SOA rivendell
2	0.005183	192.168.2.1	53	192.168.2.105	64343	DNS	Standard query response SOA elrond.rivendell
3	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [SYN] Seq=0 Win=5840
4	0.005183	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [SYN, ACK] Seq=0 Ack=
5	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [ACK] Seq=1 Ack=1 Win
6	0.005183	192.168.2.105	48348	192.168.2.1	53	TCP	[TCP segment of a reassembled PDU]
7	0.006038	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [ACK] Seq=1 Ack=3 Win=5792 Len=0 TSV=29886012
8	0.006060	192.168.2.105	48348	192.168.2.1	53	DNS	Standard query IXFR rivendell
9	0.006070	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [ACK] Seq=1 Ack=78 Win=5792 Len=0 TSV=29886012
10	0.006082	192.168.2.1	53	192.168.2.105	48348	DNS	Standard query response SOA elrond.r
11	0.006094	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [ACK] Seq=78 Ack=244 Win=6912 Len=0 TSV=830639
12	0.066301	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [FIN, ACK] Seq=78 Ack
13	0.067774	192.168.2.1	53	192.168.2.105	48348	TCP	domain > 48348 [FIN, ACK] Seq=244 Ac
14	0.067977	192.168.2.105	48348	192.168.2.1	53	TCP	48348 > domain [ACK] Seq=79 Ack=245

```
▷ Flags: 0x8480 (Standard query response, No error)
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
▽ Queries
  ▷ rivendell: type IXFR, class IN
▽ Answers
  ▷ rivendell: type SOA, class IN, mname elrond.rivendell
  ▷ rivendell: type NS, class IN, ns elrond.rivendell
  ▷ elrond.rivendell: type A, class IN, addr 192.168.2.1
  ▷ galadriel.rivendell: type A, class IN, addr 192.168.2.211
  ▷ legolas.rivendell: type A, class IN, addr 192.168.2.105
  ▷ localhost.rivendell: type A, class IN, addr 127.0.0.1
  ▷ william.rivendell: type A, class IN, addr 192.168.2.114
  ▷ rivendell: type SOA, class IN, mname elrond.rivendell
```

3 way open handshake

zone transfer

*3 way closing handshake**

TCP

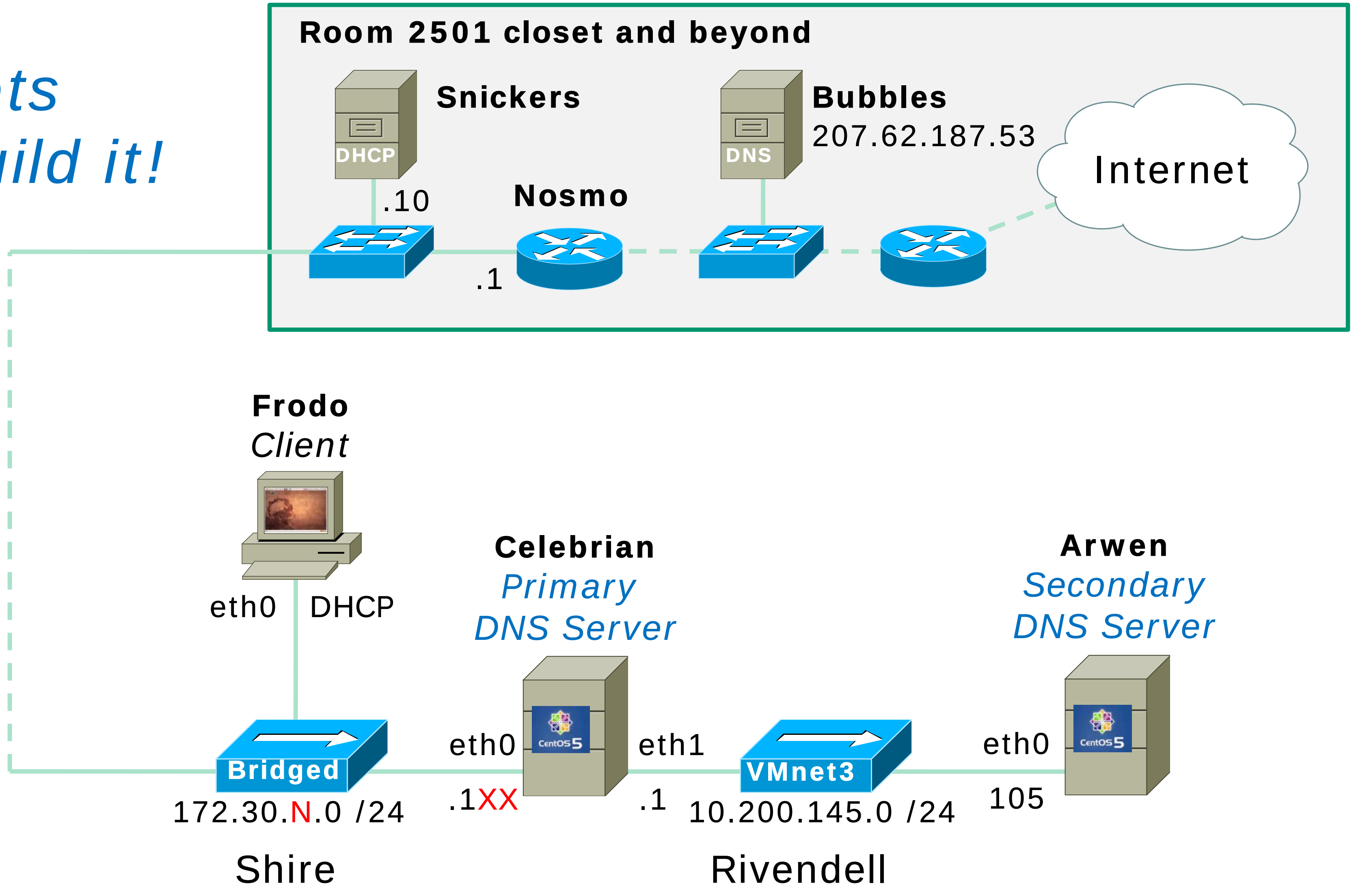
Which is then followed by a connection to TCP port 53 for the actual data transfer

Note the closing handshake is 3-way rather than 4-way. This alternative closing handshake combines step 2 (ACK) and step 3 (FIN, ACK) from 192.168.2.1 into a single step (FIN, ACK)

]

Demo
DNS
Installation

Lets build it!



Activity – Cleanup

1. On Celebrian, login as root and:

```
rm /root/bin/*
mkdir /root/packages
cd /root/bin
```

2. On Arwen, login as root and:

```
rm /root/bin/*
mkdir /root/packages
cd /root/bin
```

Clean out old scripts and make packages directory in /root

Activity – Download Celebrian scripts

1. Cable Celebrian's eth0 to the Shire network and connect with: **dhclient eth0**
2. Change to root's bin directory if not there already with: **cd /root/bin**
3. Pull down Celebrian scripts with:

   scp *logname*@opus.cabrillo.edu:/home/cis192/scripts/*celebrian /root/bin
4. Set execute permission with **chmod 700 /root/bin/***
5. Modify **update-scripts-celebrian** with your logname
6. Run script with: **./update-scripts-celebrian** *(Enter y for all ?'s)*
7. Set execute permission on all new scripts with **chmod 700 /root/bin/***
8. Release IP address with: **dhclient –r**
9. Verify files:

```
[root@celebrian bin]# ls /root/bin
do-act8A-celebrian       set-forwarding-centos  set-route-centos
init-network-centos      set-gateway-centos     show-network-centos
restart-network-centos   set-hostname-centos    update-scripts-celebrian
set-dns-centos           set-interface-centos
[root@celebrian bin]#

[root@celebrian bin]# ls /root/packages/{bind*,caching*}
/root/packages/bind-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/bind-libs-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/bind-utils-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/caching-nameserver-9.3.6-4.P1.el5_4.2.i386.rpm
[root@celebrian bin]#
```

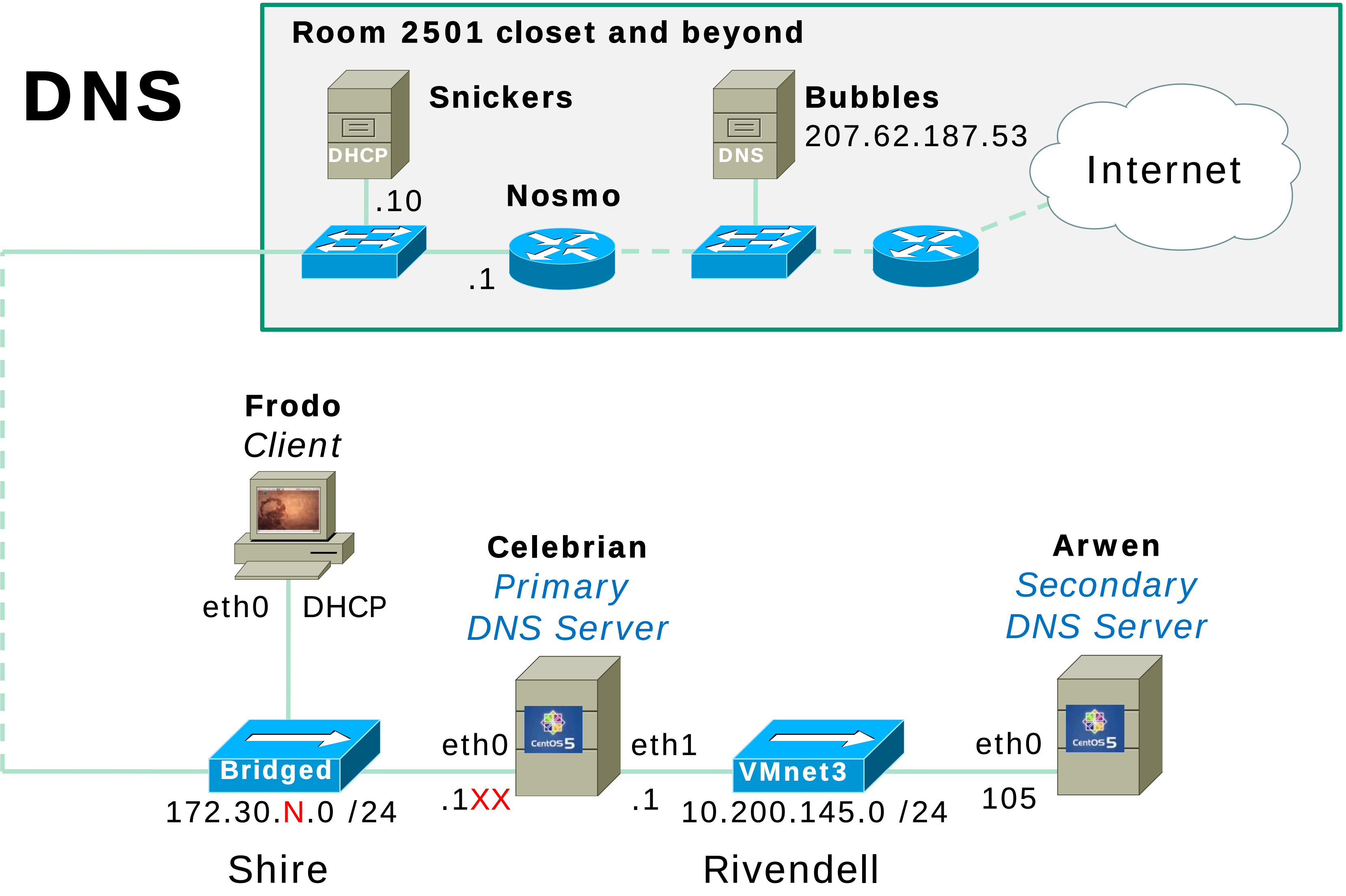
Activity – Download Arwen scripts

1. Cable Celebrian's eth0 to the Shire network and connect with: **dhclient eth0**
2. Change to root's bin directory if not there already with: **cd /root/bin**
3. Pull down Celebrian scripts with:

   scp *logname*@opus.cabrillo.edu:/home/cis192/scripts/*arwen /root/bin
4. Set execute permission with **chmod 700 /root/bin/***
5. Modify **update-scripts-arwen** with your logname
6. Run script with: **./update-scripts-arwen** *(Enter y for all ?'s)*
7. Set execute permission on all new scripts with **chmod 700 /root/bin/***
8. Release IP address with: **dhclient –r**
9. Verify files:

```
[root@arwen bin]# ls
do-act8A-arwen           set-forwarding-centos   set-route-centos
init-network-centos      set-gateway-centos      show-network-centos
restart-network-centos   set-hostname-centos     update-scripts-arwen
set-dns-centos           set-interface-centos
[root@arwen bin]#

[root@arwen bin]# ls /root/packages/{bind*,caching*}
/root/packages/bind-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/bind-libs-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/bind-utils-9.3.6-4.P1.el5_4.2.i386.rpm
/root/packages/caching-nameserver-9.3.6-4.P1.el5_4.2.i386.rpm
[root@arwen bin]#
```

DNS

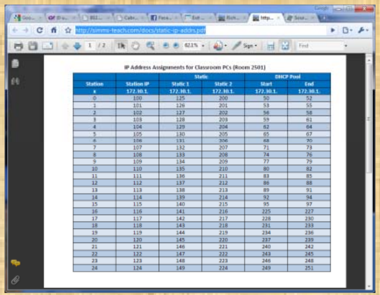


Verify correct cabling on Celebrian and Arwen

Customize do-act8A-celebrian script

```
[root@celebrian bin]# head -15 do-act8A-celebrian
!/bin/bash
#
# Do Activity 8A on Celebrian
#

# Modify the following lines for static IP your workstation
# using http://simms-teach.com/docs/static-ip-addrs.pdf

# Station-00 in classroom
static1=172.30.1.1XX
router=172.30.1.1
# CIS-Lab-06 in lab
#static1=172.30.4.131
#router=172.30.4.1

[root@celebrian bin]#
```

Modify to your unique static IP address from



http://simms-teach.com/docs/static-ip-addrs.pdf

IP Address Assignments for Classroom PCs (Room 2501)

		Static		DHCP Pool	
Station	Station IP	Static 1	Static 2	Start	End
x	172.30.1.	172.30.1.	172.30.1.	172.30.1.	172.30.1.
0	100	125	200	50	52
1	101	126	201	53	55
2	102	127	202	56	58
3	103	128	203	59	61
4	104	129	204	62	64
5	105	130	205	65	67
6	106	131	206	68	70
7	107	132	207	71	73
8	108	133	208	74	76
9	109	134	209	77	79
10	110	135	210	80	82
11	111	136	211	83	85
12	112	137	212	86	88
13	113	138	213	89	91
14	114	139	214	92	94
15	115	140	215	95	97
16	116	141	216	225	227
17	117	142	217	228	230
18	118	143	218	231	233
19	119	144	219	234	236
20	120	145	220	237	239
21	121	146	221	240	242
22	122	147	222	243	245
23	123	148	223	246	248
24	124	149	224	249	251

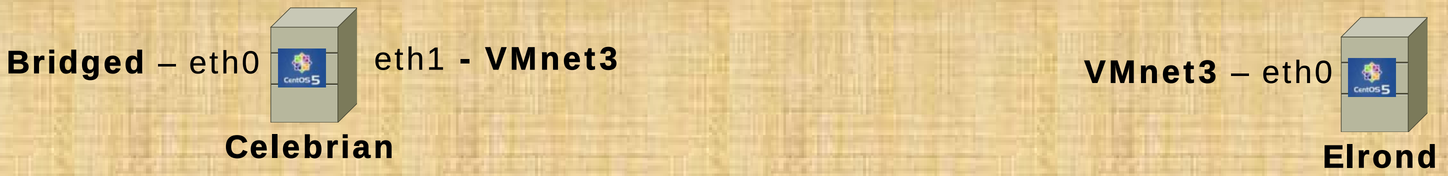
Activity – Peer Walkthrough

The power of a second set of eyes is invaluable!

1. Pair up with another student

2. Verify **Celebrian** and **Arwen** VMs:
   - □ Logged on as root
   - □ Scripts are in root's bin directory
   - □ RPMs are in root's packages directory
   - □ The "do-*" scripts match the VM's name
   - □ The other scripts match VM's distro (CentOS)
   - □ Execute permission has been set on all scripts
   - □ Cabling is correct

3. Verify the do-act8A-celebrian script on **Celebrian** has the correct eth0 IP address



Bridged – eth0 eth1 - **VMnet3**

Celebrian

VMnet3 – eth0

Elrond

Activity 8A

1. On Celebrian, in /root/bin, use:

   ./do-act8A-celebrian

2. On Arwen, in /root/bin, use:

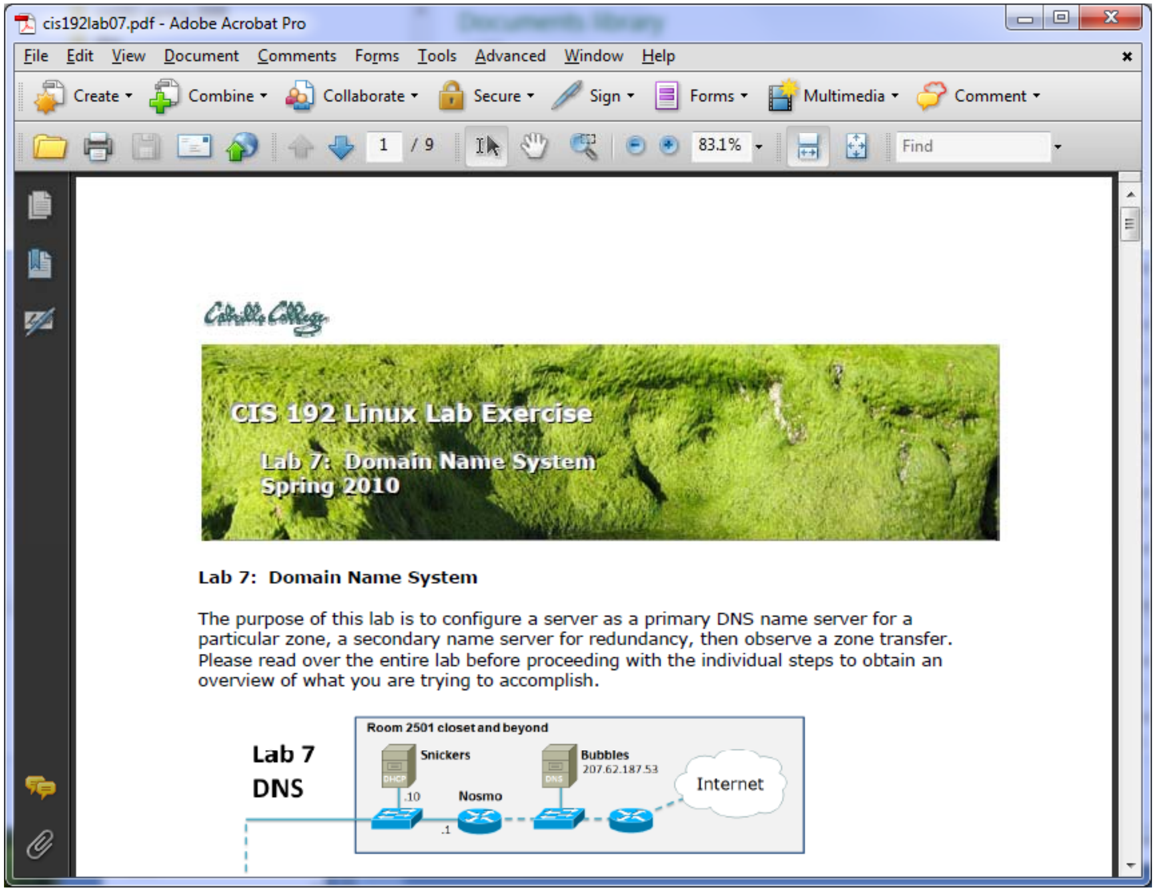
   ./do-act8A-arwen

Use Enter key to confirm and continue

*When prompted to **restart the network**, type y to confirm*

Lab 7

Lab 7



cis192lab07.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Create Combine Collaborate Secure Sign Forms Multimedia Comment
1 / 9
83.1%
Find

CIS 192 Linux Lab Exercise

Lab 7: Domain Name System
Spring 2010

Lab 7: Domain Name System

The purpose of this lab is to configure a server as a primary DNS name server for a particular zone, a secondary name server for redundancy, then observe a zone transfer. Please read over the entire lab before proceeding with the individual steps to obtain an overview of what you are trying to accomplish.

Wrap

New commands, daemons:

named	DNS daemon
host	For testing DNS
dig	DNS information
nslookup	Being phased out
rndc reload	Reload DNS configuration files

setenforce
getenforce
setsebool
getsebool
sestatus

Configuration files

/etc/named.conf
/var/named/*
/etc/resolv.conf
/etc/nsswitch.conf
/etc/hosts

Next Class (after Spring Break)

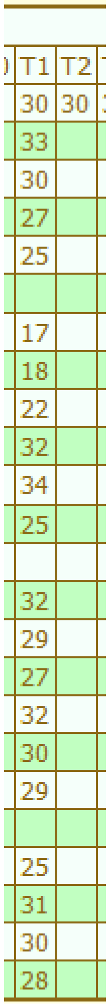
Assignment: Check Calendar Page
http://simms-teach.com/cis192calendar.php

Lab 7 due

Quiz questions for next class:

- What two packages must be installed to setup a name server with caching?
- What is the purpose of a PTR record?
- How does the serial number effect zone transfers?

A Pizza Bribe for This Test

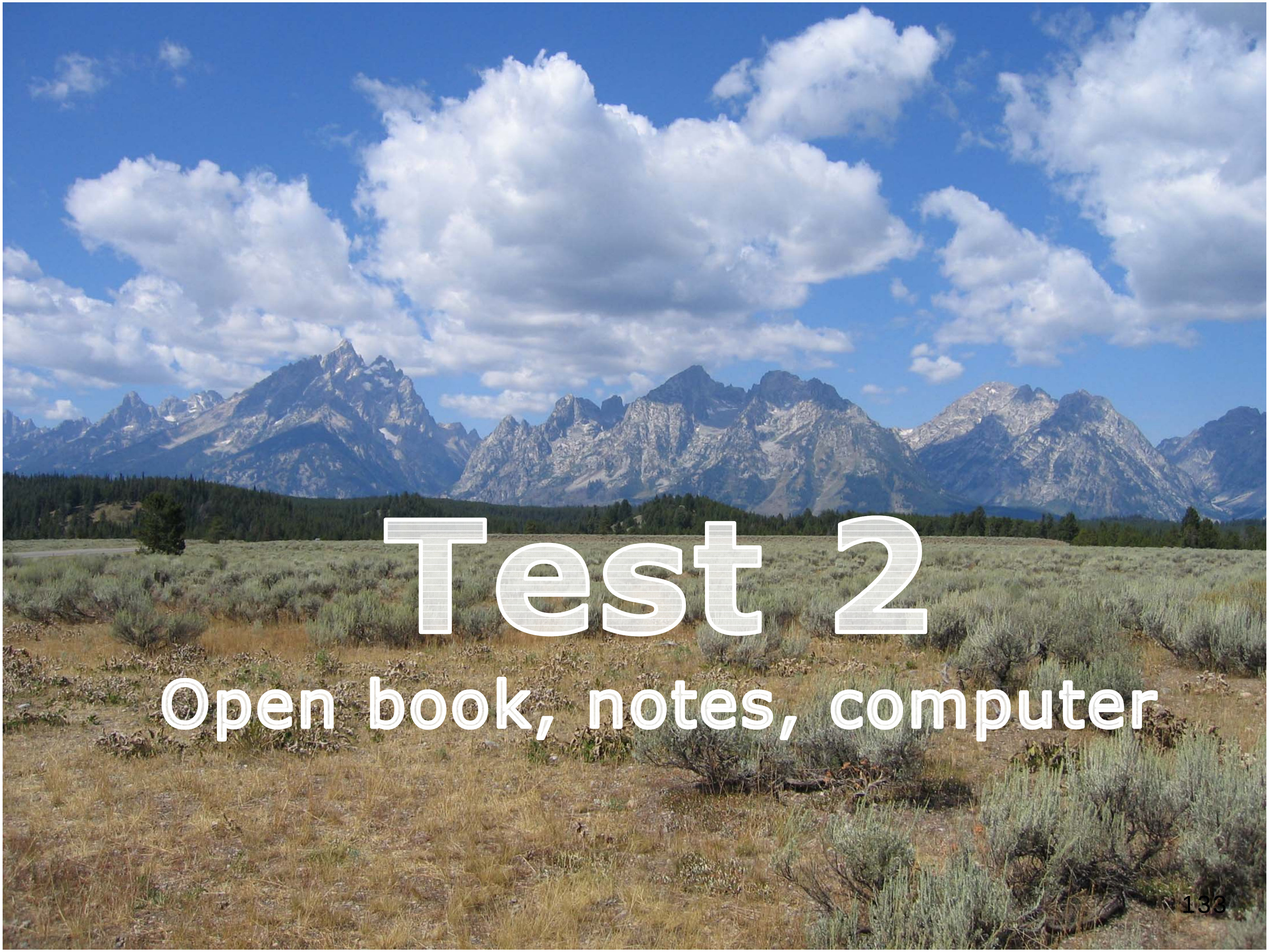


T1	T2
30	30
33	
30	
27	
25	
17	
18	
22	
32	
34	
25	
32	
29	
27	
32	
30	
29	
25	
31	
30	
28	

T1 average score = 27.80

The Pizza Bribe is as follows:

If T2 average > 27.80 then **PIZZA for the CLASS**



Test 2

Open book, notes, computer

Backup

dig simms-teach.com (com. servers)

```
[root@elrond ~]# dig +norec +noques +nostats +nocmd simms-teach.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16548
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 0

;; AUTHORITY SECTION:
com.                    172798  IN      NS      G.GTLD-SERVERS.NET.
com.                    172798  IN      NS      M.GTLD-SERVERS.NET.
com.                    172798  IN      NS      K.GTLD-SERVERS.NET.
com.                    172798  IN      NS      A.GTLD-SERVERS.NET.
com.                    172798  IN      NS      C.GTLD-SERVERS.NET.
com.                    172798  IN      NS      L.GTLD-SERVERS.NET.
com.                    172798  IN      NS      J.GTLD-SERVERS.NET.
com.                    172798  IN      NS      H.GTLD-SERVERS.NET.
com.                    172798  IN      NS      B.GTLD-SERVERS.NET.
com.                    172798  IN      NS      I.GTLD-SERVERS.NET.
com.                    172798  IN      NS      E.GTLD-SERVERS.NET.
com.                    172798  IN      NS      F.GTLD-SERVERS.NET.
com.                    172798  IN      NS      D.GTLD-SERVERS.NET.
```

NS = Authoritative Name Server record

IN = Internet Domain Names

dig simms-teach.com (simms-teach.com. servers)

```
[root@elrond ~]# dig +norec +noques +nostats +nocmd simms-teach.com @A.GTLD-SERVERS.NET.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40276
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 3

;; AUTHORITY SECTION:
simms-teach.com.        172800  IN      NS      ns1.dreamhost.com.
simms-teach.com.        172800  IN      NS      ns2.dreamhost.com.
simms-teach.com.        172800  IN      NS      ns3.dreamhost.com.

;; ADDITIONAL SECTION:
ns1.dreamhost.com.      172800  IN      A       66.33.206.206
ns2.dreamhost.com.      172800  IN      A       208.96.10.221
ns3.dreamhost.com.      172800  IN      A       66.33.216.216

[root@elrond ~]#
```

dig simms-teach.com (ANSWER section received)

```
[root@elrond ~]# dig +norec +noques +nostats +nocmd simms-teach.com @ns1.dreamhost.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60986
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
simms-teach.com.        14400   IN      A       208.113.161.13

[root@elrond ~]#
```

```
[root@elrond ~]# ping -c2 simms-teach.com
PING simms-teach.com (208.113.161.13) 56(84) bytes of data.
64 bytes from apache2-zoo.nehi.dreamhost.com (208.113.161.13): icmp_seq=1 ttl=56 time=26.1 ms
64 bytes from apache2-zoo.nehi.dreamhost.com (208.113.161.13): icmp_seq=2 ttl=56 time=25.9 ms

--- simms-teach.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 25.973/26.078/26.184/0.192 ms
[root@elrond ~]#
```

An example of what it is like to be a resolver doing a reverse lookup using the dig command

dig 9.186.62.207.in-addr.arpa

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd 9.186.62.207.in-addr.arpa
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26350
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 5

;; AUTHORITY SECTION:
.                       518387  IN      NS      I.ROOT-SERVERS.NET.
.                       518387  IN      NS      C.ROOT-SERVERS.NET.
.                       518387  IN      NS      E.ROOT-SERVERS.NET.
.                       518387  IN      NS      F.ROOT-SERVERS.NET.
.                       518387  IN      NS      K.ROOT-SERVERS.NET.
.                       518387  IN      NS      A.ROOT-SERVERS.NET.
.                       518387  IN      NS      L.ROOT-SERVERS.NET.
.                       518387  IN      NS      H.ROOT-SERVERS.NET.
.                       518387  IN      NS      M.ROOT-SERVERS.NET.
.                       518387  IN      NS      B.ROOT-SERVERS.NET.
.                       518387  IN      NS      G.ROOT-SERVERS.NET.
.                       518387  IN      NS      D.ROOT-SERVERS.NET.
.                       518387  IN      NS      J.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     604782  IN      A       198.41.0.4
A.ROOT-SERVERS.NET.     604787  IN      AAAA    2001:503:ba3e::2:30
E.ROOT-SERVERS.NET.     604787  IN      A       192.203.230.10
M.ROOT-SERVERS.NET.     604787  IN      A       202.12.27.33
M.ROOT-SERVERS.NET.     604782  IN      AAAA    2001:dc3::35

[root@elrond ~]#
```

dig 9.186.62.207.in-addr.arpa

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd 9.186.62.207.in-addr.arpa @A.ROOT-
   SERVERS.NET.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12044
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 0

;; AUTHORITY SECTION:
207.in-addr.arpa.       86400   IN      NS      X.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      BASIL.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      HENNA.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      Y.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      CHIA.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      DILL.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      Z.ARIN.NET.
207.in-addr.arpa.       86400   IN      NS      INDIGO.ARIN.NET.

[root@elrond ~]#
```

dig 9.186.62.207.in-addr.arpa

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd 9.186.62.207.in-addr.arpa
  @BASIL.ARIN.NET.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56550
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 0

;; AUTHORITY SECTION:
62.207.in-addr.arpa.    86400   IN      NS      ns2.csu.net.
62.207.in-addr.arpa.    86400   IN      NS      ns1.csu.net.

[root@elrond ~]#
```

dig 9.186.62.207.in-addr.arpa

```
[root@elrond ~]# dig +norecurse +noques +nostats +nocmd 9.186.62.207.in-addr.arpa @ns1.csu.net
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58855
;; flags: qr aa ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; AUTHORITY SECTION:
186.62.207.in-addr.arpa. 28800  IN      SOA     buttercup.cabrillo.edu.
  hostmaster.cabrillo.edu. 2004062137 3600 1800 604800 28800

[root@elrond ~]#
```

Firewall and DNS port

*This command **inserts** a new rule on the custom firewall chain on the primary to allow new UDP port 53 requests*

line number to insert before

Name of chain

```
[root@elrond ~]# iptables -I RH-Firewall-1-INPUT 9 -m state
--state NEW -m udp -p udp --dport 53 -j ACCEPT
```

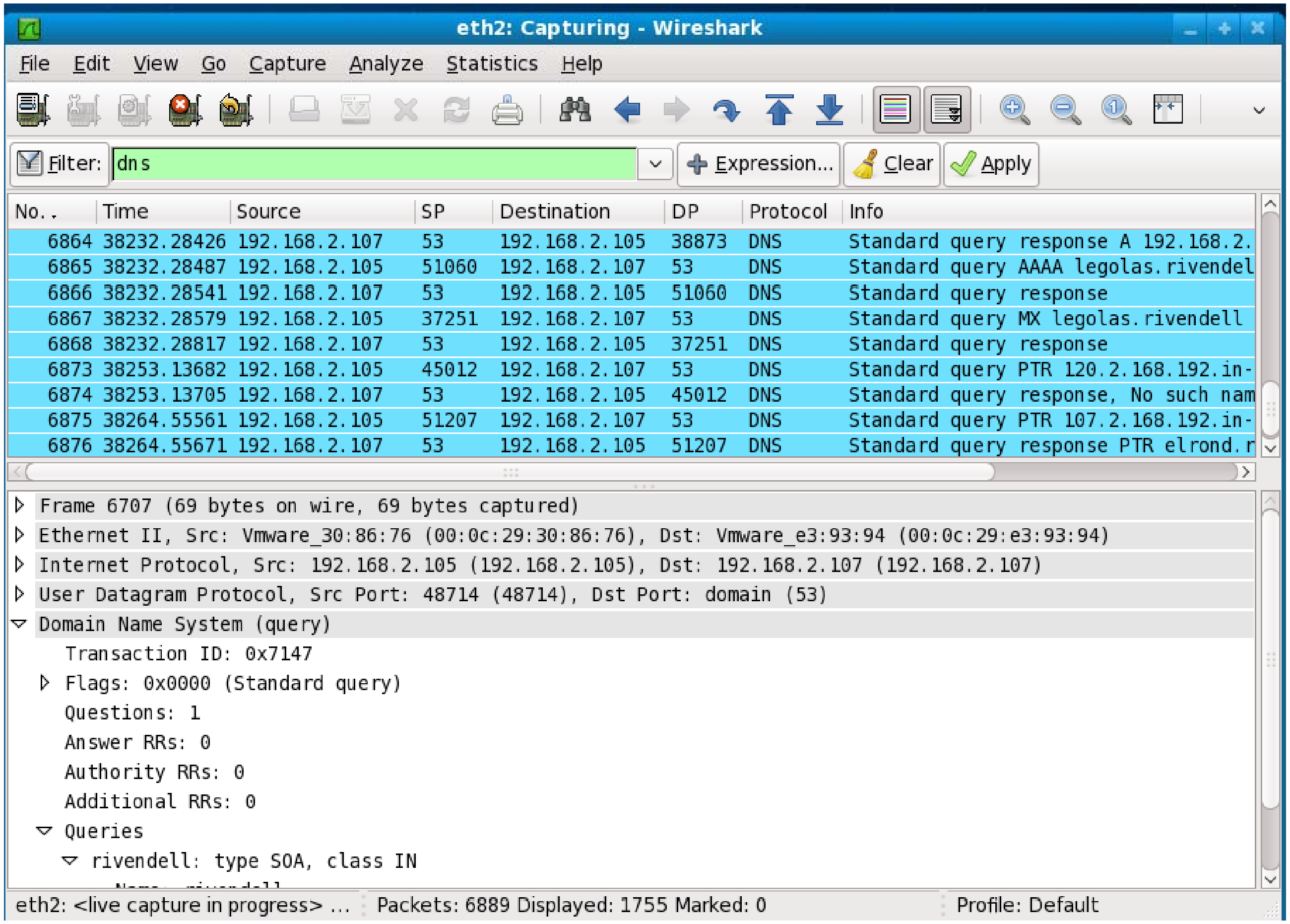
-m	specifies match modules to use
-p	specified protocol to match
-I	to insert a new rule
--state NEW	for new (not yet established) connections
--dport	for the destination port

Modified firewall on CentOS (Red Hat) now allows DNS requests

```
[root@elrond ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     esp  --  anywhere             anywhere
ACCEPT     ah   --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251         udp dpt:mdns
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ipp
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ipp
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere            state NEW udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited
[root@elrond ~]#
```

UDP port 53 is open

Modified firewall on CentOS (Red Hat) primary now allows DNS requests



Filter: dns

```
No..  Time         Source         SP     Destination    DP     Protocol  Info
 6864 38232.28426 192.168.2.107  53     192.168.2.105  38873  DNS       Standard query response A 192.168.2.
 6865 38232.28487 192.168.2.105  51060  192.168.2.107  53     DNS       Standard query AAAA legolas.rivendel
 6866 38232.28541 192.168.2.107  53     192.168.2.105  51060  DNS       Standard query response
 6867 38232.28579 192.168.2.105  37251  192.168.2.107  53     DNS       Standard query MX legolas.rivendell
 6868 38232.28817 192.168.2.107  53     192.168.2.105  37251  DNS       Standard query response
 6873 38253.13682 192.168.2.105  45012  192.168.2.107  53     DNS       Standard query PTR 120.2.168.192.in-
 6874 38253.13705 192.168.2.107  53     192.168.2.105  45012  DNS       Standard query response, No such nam
 6875 38264.55561 192.168.2.105  51207  192.168.2.107  53     DNS       Standard query PTR 107.2.168.192.in-
 6876 38264.55671 192.168.2.107  53     192.168.2.105  51207  DNS       Standard query response PTR elrond.r
```

```
▷ Frame 6707 (69 bytes on wire, 69 bytes captured)
▷ Ethernet II, Src: Vmware_30:86:76 (00:0c:29:30:86:76), Dst: Vmware_e3:93:94 (00:0c:29:e3:93:94)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.107 (192.168.2.107)
▷ User Datagram Protocol, Src Port: 48714 (48714), Dst Port: domain (53)
▽ Domain Name System (query)
    Transaction ID: 0x7147
  ▷ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ rivendell: type SOA, class IN
        Name: rivendell
```

eth2: <live capture in progress> ... Packets: 6889 Displayed: 1755 Marked: 0 Profile: Default

UDP port 53 is open

DNS Trobleshooting

Lab 7 Troubleshooting

Problem: primary to secondary transfer failing

From /var/log/messages:

```
Apr  6 06:39:33 legolas named[16429]: zone rivendell/IN: Transfer
started.
Apr  6 06:39:33 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: connected using 192.168.2.105#54165
Apr  6 06:39:33 legolas named[16429]: dumping primary file: tmp-
UjD7J9kLlr: open: permission denied
Apr  6 06:39:33 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: failed while receiving responses: permission denied
Apr  6 06:39:33 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: end of transfer
```

Solution:

Enable named to create new files on secondary:

1. Run **lokkit** on secondary and change SELinux setting from Enforcing to Permissive
2. Use **chmod 770 /var/named** on secondary

Lab 7 Troubleshooting

Problem: primary to secondary transfer failing

From /var/log/messages:

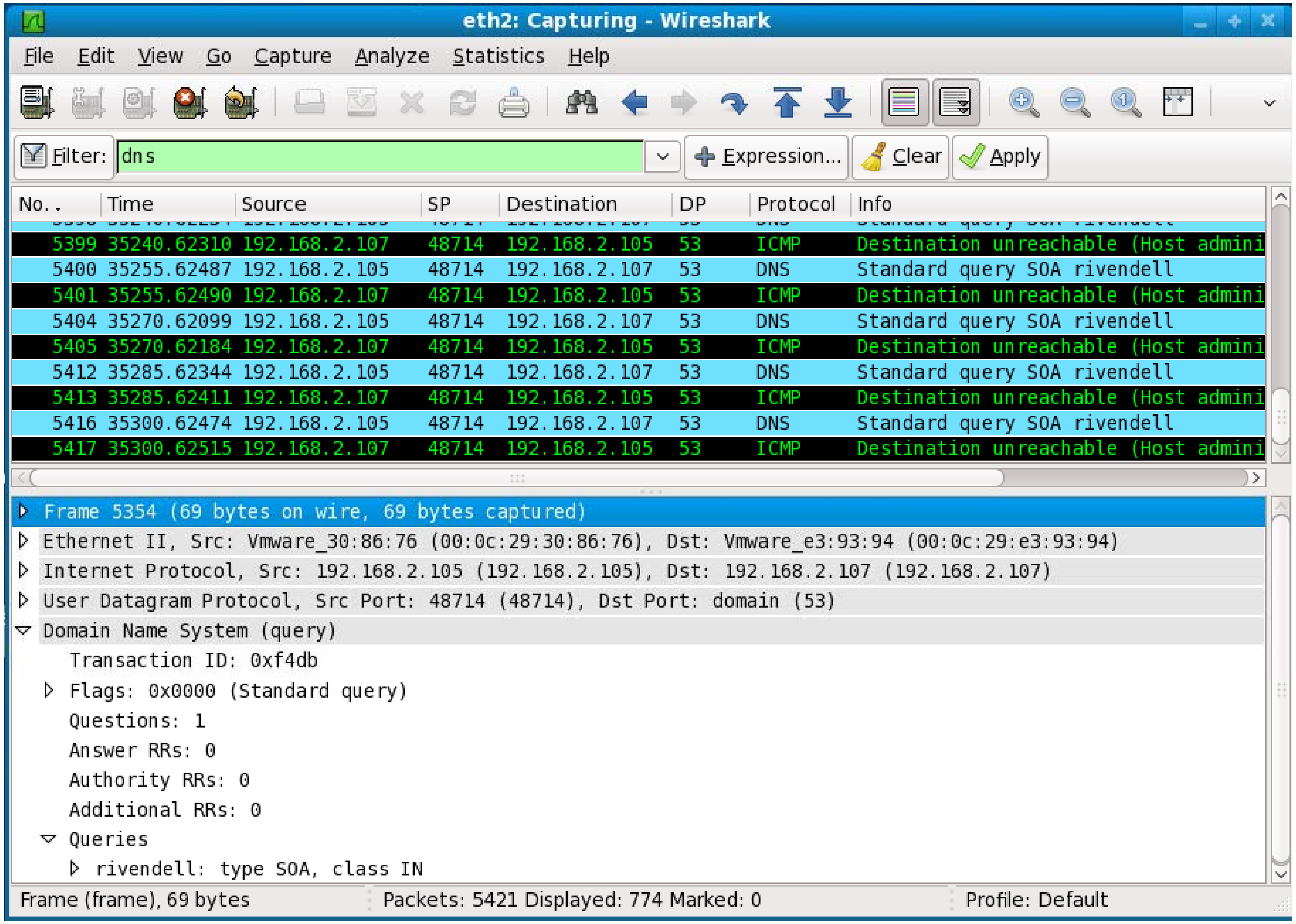
```
Apr  6 07:01:15 legolas named[16429]: zone rivendell/IN: refresh:
retry limit for primary 192.168.2.107#53 exceeded (source 0.0.0.0#0)
Apr  6 07:01:15 legolas named[16429]: zone rivendell/IN: Transfer
started.
Apr  6 07:01:15 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: failed to connect: host unreachable
Apr  6 07:01:15 legolas named[16429]: transfer of 'rivendell/IN' from
192.168.2.107#53: end of transfer
```

Solution:

Firewall on primary is blocking connection by secondary for transfer

1. Run **lokkit** on primary and disable firewall or
2. Open port UDP port 53 on primary

Zone transfer failing when blocked by firewall on primary

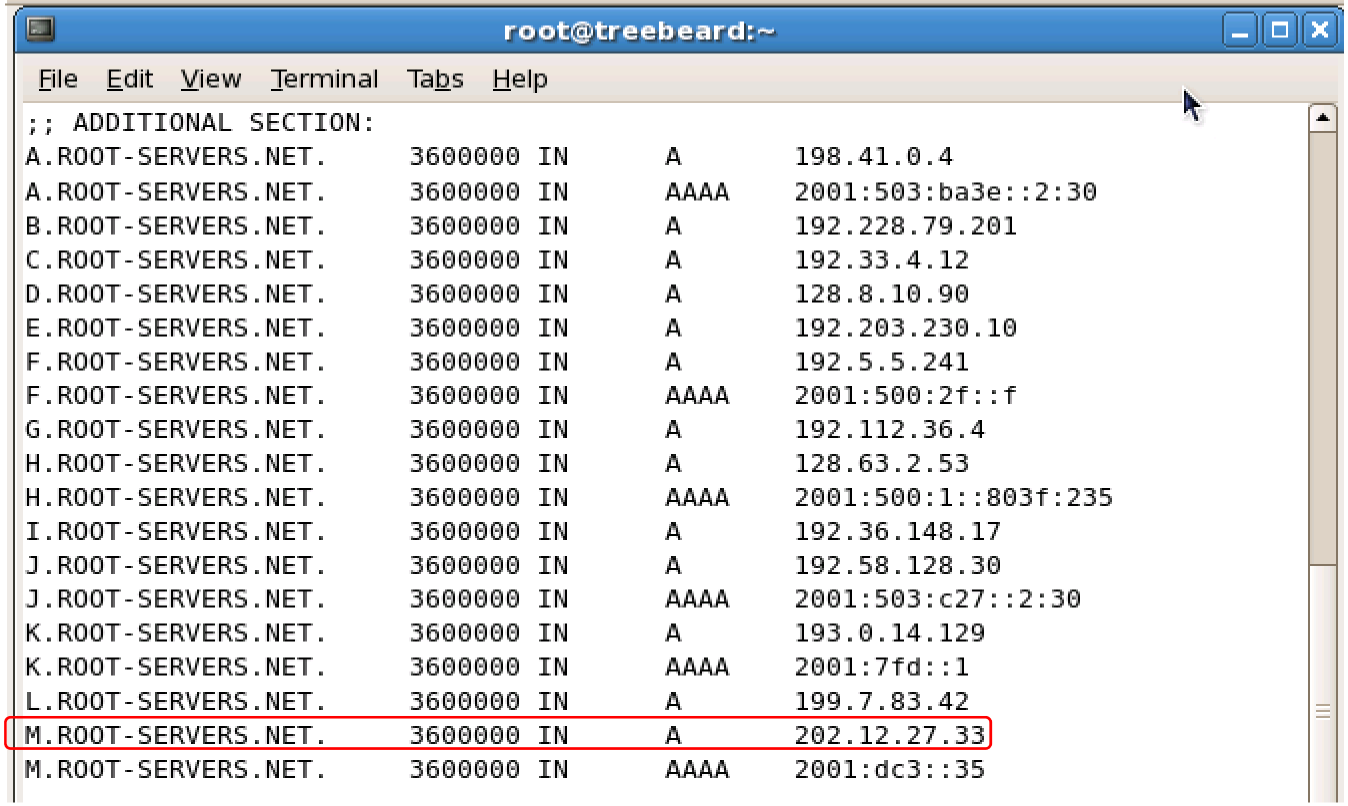

eth2: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

Filter: dns

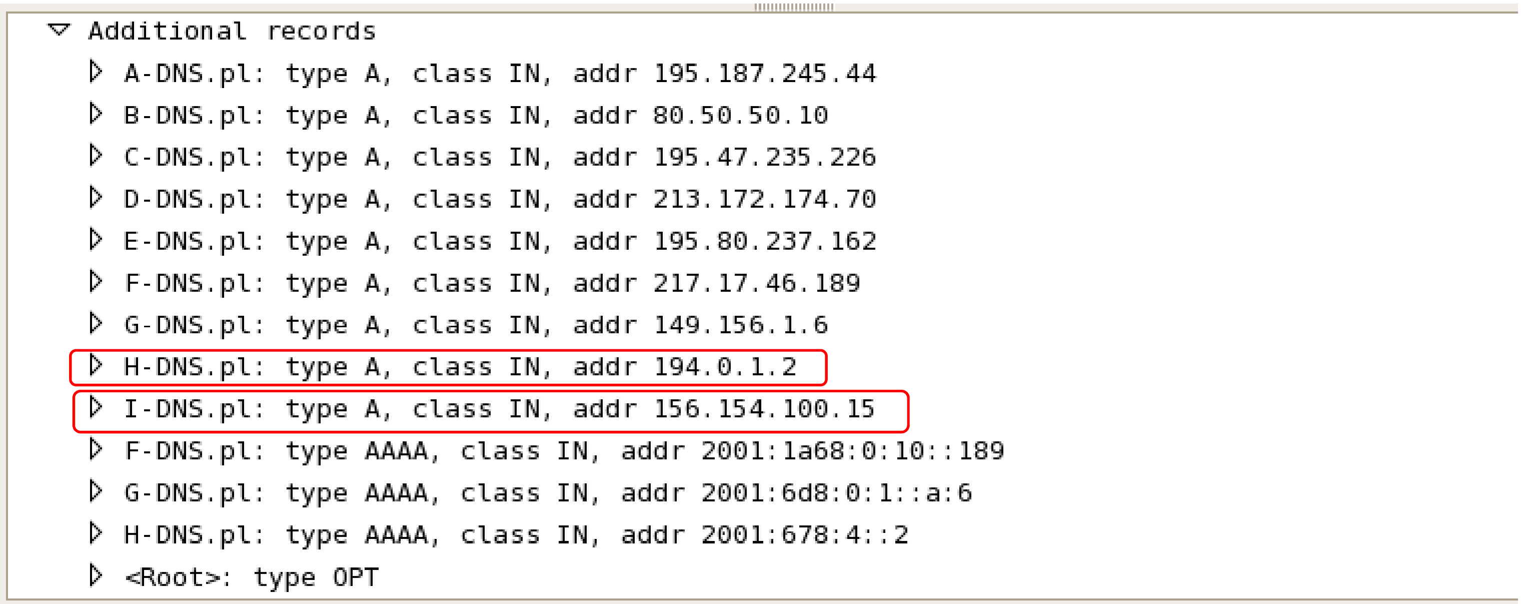
```
No. .  Time         Source         SP     Destination    DP   Protocol  Info
 5399 35240.62310 192.168.2.107  48714  192.168.2.105  53   ICMP      Destination unreachable (Host admini
 5400 35255.62487 192.168.2.105  48714  192.168.2.107  53   DNS       Standard query SOA rivendell
 5401 35255.62490 192.168.2.107  48714  192.168.2.105  53   ICMP      Destination unreachable (Host admini
 5404 35270.62099 192.168.2.105  48714  192.168.2.107  53   DNS       Standard query SOA rivendell
 5405 35270.62184 192.168.2.107  48714  192.168.2.105  53   ICMP      Destination unreachable (Host admini
 5412 35285.62344 192.168.2.105  48714  192.168.2.107  53   DNS       Standard query SOA rivendell
 5413 35285.62411 192.168.2.107  48714  192.168.2.105  53   ICMP      Destination unreachable (Host admini
 5416 35300.62474 192.168.2.105  48714  192.168.2.107  53   DNS       Standard query SOA rivendell
 5417 35300.62515 192.168.2.107  48714  192.168.2.105  53   ICMP      Destination unreachable (Host admini
```

```
▷ Frame 5354 (69 bytes on wire, 69 bytes captured)
▷ Ethernet II, Src: Vmware_30:86:76 (00:0c:29:30:86:76), Dst: Vmware_e3:93:94 (00:0c:29:e3:93:94)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.107 (192.168.2.107)
▷ User Datagram Protocol, Src Port: 48714 (48714), Dst Port: domain (53)
▽ Domain Name System (query)
    Transaction ID: 0xf4db
  ▷ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▷ rivendell: type SOA, class IN
```

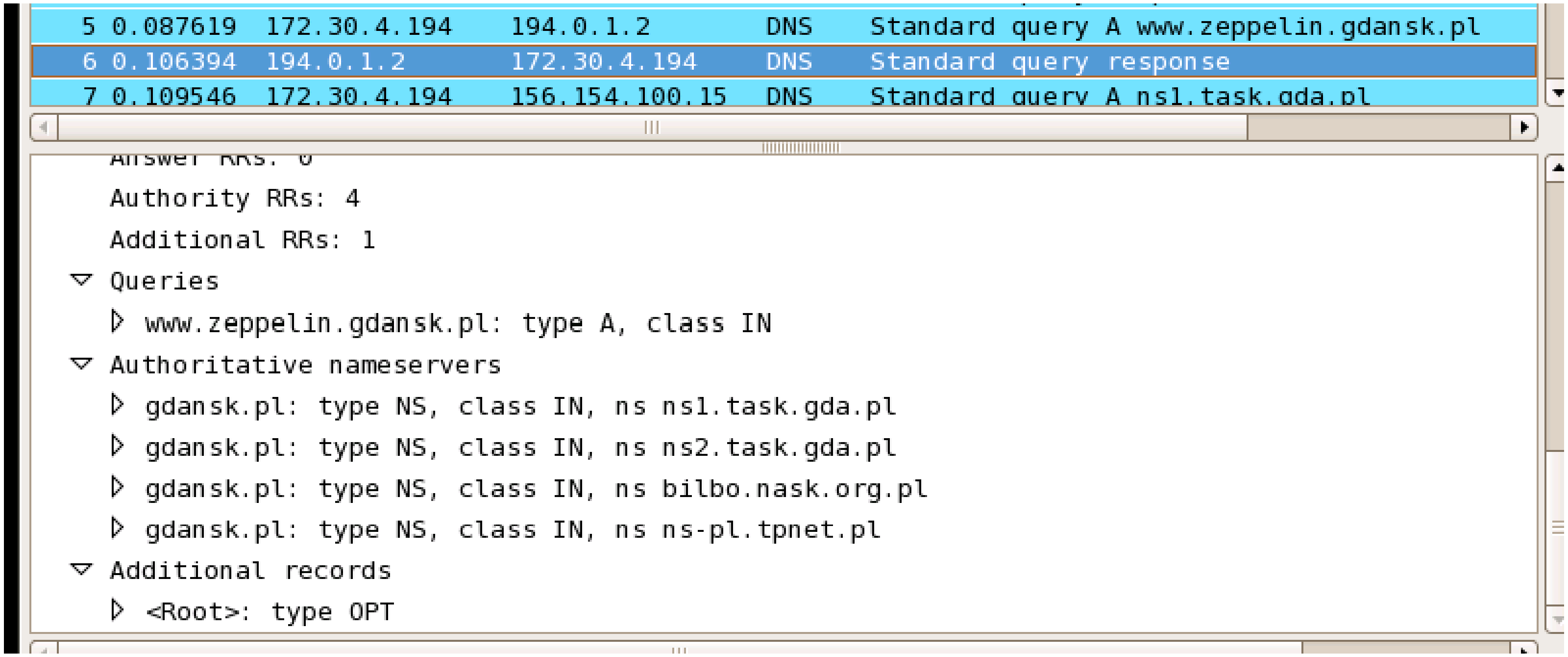
Frame (frame), 69 bytes   Packets: 5421 Displayed: 774 Marked: 0   Profile: Default *seedling (172.30.4.194): ping -c2 www.zeppelin.gdansk.pl*



```
;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.      3600000 IN      A       198.41.0.4
A.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:503:ba3e::2:30
B.ROOT-SERVERS.NET.      3600000 IN      A       192.228.79.201
C.ROOT-SERVERS.NET.      3600000 IN      A       192.33.4.12
D.ROOT-SERVERS.NET.      3600000 IN      A       128.8.10.90
E.ROOT-SERVERS.NET.      3600000 IN      A       192.203.230.10
F.ROOT-SERVERS.NET.      3600000 IN      A       192.5.5.241
F.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:500:2f::f
G.ROOT-SERVERS.NET.      3600000 IN      A       192.112.36.4
H.ROOT-SERVERS.NET.      3600000 IN      A       128.63.2.53
H.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:500:1::803f:235
I.ROOT-SERVERS.NET.      3600000 IN      A       192.36.148.17
J.ROOT-SERVERS.NET.      3600000 IN      A       192.58.128.30
J.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:503:c27::2:30
K.ROOT-SERVERS.NET.      3600000 IN      A       193.0.14.129
K.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:7fd::1
L.ROOT-SERVERS.NET.      3600000 IN      A       199.7.83.42
M.ROOT-SERVERS.NET.      3600000 IN      A       202.12.27.33
M.ROOT-SERVERS.NET.      3600000 IN      AAAA    2001:dc3::35
```



```
▽ Additional records
   ▷ A-DNS.pl: type A, class IN, addr 195.187.245.44
   ▷ B-DNS.pl: type A, class IN, addr 80.50.50.10
   ▷ C-DNS.pl: type A, class IN, addr 195.47.235.226
   ▷ D-DNS.pl: type A, class IN, addr 213.172.174.70
   ▷ E-DNS.pl: type A, class IN, addr 195.80.237.162
   ▷ F-DNS.pl: type A, class IN, addr 217.17.46.189
   ▷ G-DNS.pl: type A, class IN, addr 149.156.1.6
   ▷ H-DNS.pl: type A, class IN, addr 194.0.1.2
   ▷ I-DNS.pl: type A, class IN, addr 156.154.100.15
   ▷ F-DNS.pl: type AAAA, class IN, addr 2001:1a68:0:10::189
   ▷ G-DNS.pl: type AAAA, class IN, addr 2001:6d8:0:1::a:6
   ▷ H-DNS.pl: type AAAA, class IN, addr 2001:678:4::2
   ▷ <Root>: type OPT
```



```
 5 0.087619  172.30.4.194    194.0.1.2       DNS   Standard query A www.zeppelin.gdansk.pl
 6 0.106394  194.0.1.2       172.30.4.194    DNS   Standard query response
 7 0.109546  172.30.4.194    156.154.100.15  DNS   Standard query A ns1.task.gda.pl
```

```
    Answer RRs: 0
    Authority RRs: 4
    Additional RRs: 1
 ▽ Queries
   ▷ www.zeppelin.gdansk.pl: type A, class IN
 ▽ Authoritative nameservers
   ▷ gdansk.pl: type NS, class IN, ns ns1.task.gda.pl
   ▷ gdansk.pl: type NS, class IN, ns ns2.task.gda.pl
   ▷ gdansk.pl: type NS, class IN, ns bilbo.nask.org.pl
   ▷ gdansk.pl: type NS, class IN, ns ns-pl.tpnet.pl
 ▽ Additional records
   ▷ <Root>: type OPT
```

Lab 7 Troubleshooting

Problem: primary to secondary transfer failing

From /var/log/messages:

```
Apr 13 09:12:49 legolas named[12584]: listening on IPv4 interface lo, 127.0.0.1#53
Apr 13 09:12:49 legolas named[12584]: listening on IPv4 interface eth0,
192.168.2.105#53
Apr 13 09:12:49 legolas named[12584]: command channel listening on 127.0.0.1#953
Apr 13 09:12:49 legolas named[12584]: the working directory is not writable
Apr 13 09:12:49 legolas named[12584]: zone 0.0.127.in-addr.arpa/IN: loaded serial
1997022700
Apr 13 09:12:49 legolas named[12584]: zone localhost/IN: loaded serial 42
Apr 13 09:12:49 legolas named[12584]: running
```

Solution:

Change permissions form 750 to 770 so named can create files in /var/named:

1. Use **chmod 770 /var/named** on secondary