Lecture 16

**DNS-Caching Server-land DNS Server (Most Important Topic)**

DNS

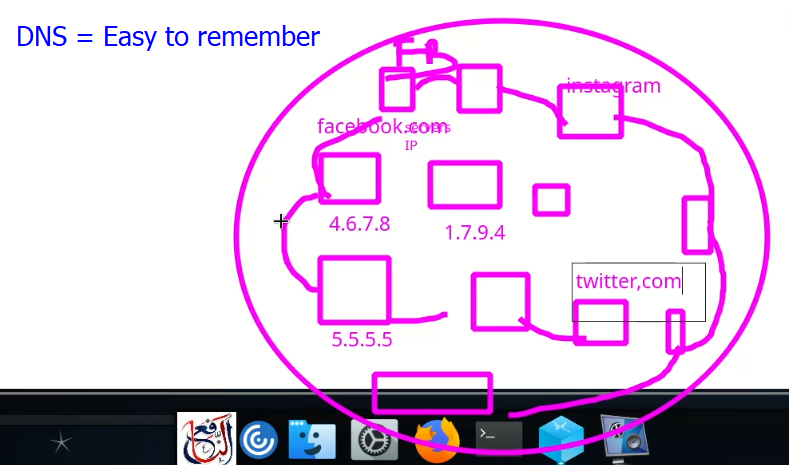
Domain Name System / Domain Name Service

* Name to IP resolution
* Name se IP milta hai
* Easy to remember

DNS stands for Domain Name System. It is a system used to translate human-readable domain names (such as google.com) into IP addresses that can be understood by computers.

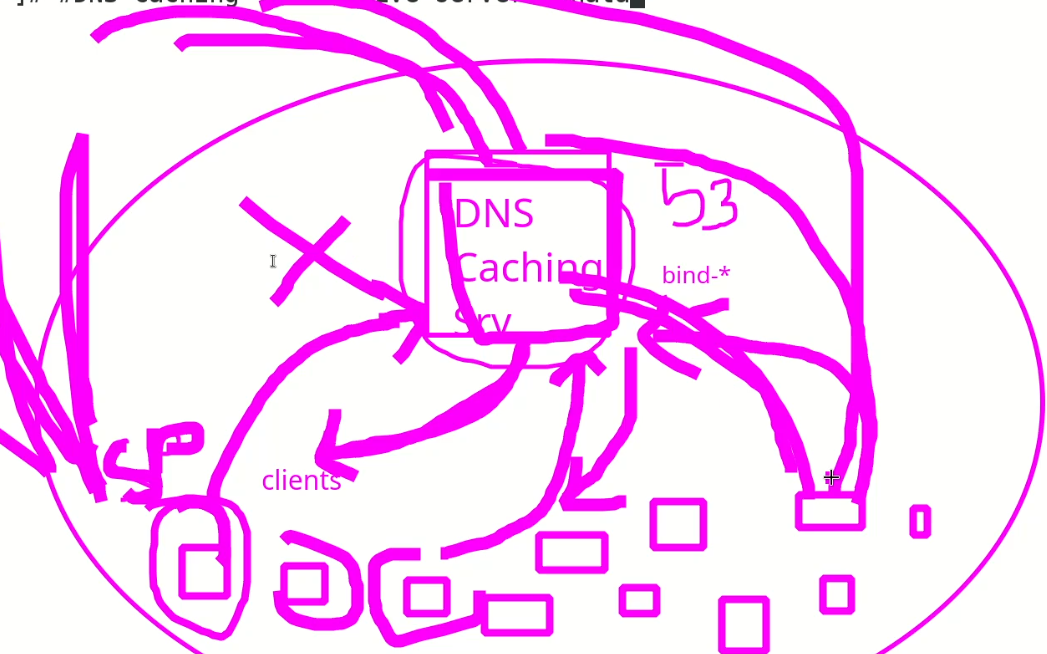
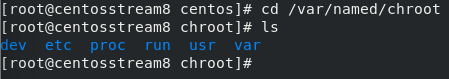
*When a user types in a domain name in a web browser, the browser sends a request to a DNS server to resolve the domain name into an IP address. The DNS server then looks up the IP address associated with that domain name and returns it to the browser. The browser can then use the IP address to establish a connection with the web server hosting the website associated with that domain name.*

The DNS system is hierarchical, with a few top-level domains (such as .com, .org, and .net) at the top, followed by second-level domains (such as google.com), and subdomains (such as mail.google.com). The DNS system is an essential component of the internet infrastructure, enabling users to access websites and other internet services using easy-to-remember domain names instead of numeric IP addresses.

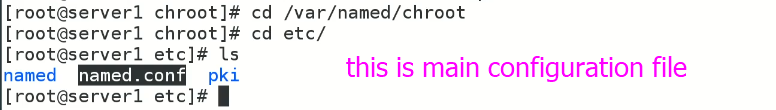
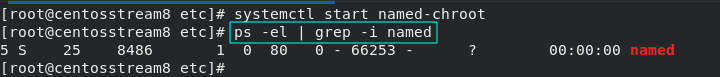
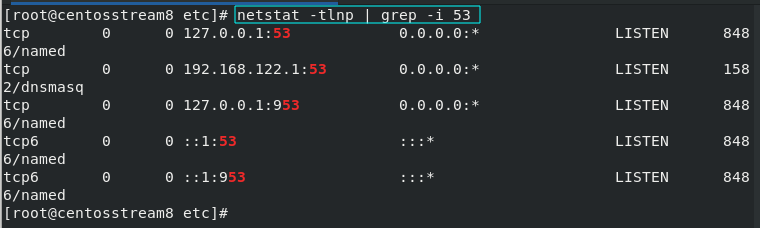
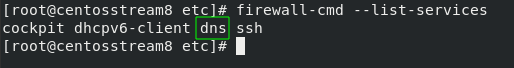
* 
* DNS (Domain Name System) uses two main ports, UDP (User Datagram Protocol) port 53 and TCP (Transmission Control Protocol) port 53.
* UDP port 53 is used for DNS queries, which are typically small and can be sent and received quickly. DNS queries are usually less than 512 bytes in size, so they fit well within the 1,500-byte maximum size of a UDP packet.
* TCP port 53 is used for larger DNS responses that cannot fit within a single UDP packet. TCP is a reliable and connection-oriented protocol, so it ensures that all data is received by the receiver without errors. DNS over TCP is usually used for zone transfers and large DNS record queries.
* However, the use of TCP for DNS is less common than the use of UDP because it involves more overhead due to its connection-oriented nature. The majority of DNS traffic uses UDP port 53.
* Top of Form
* .

We are going to create 🡪



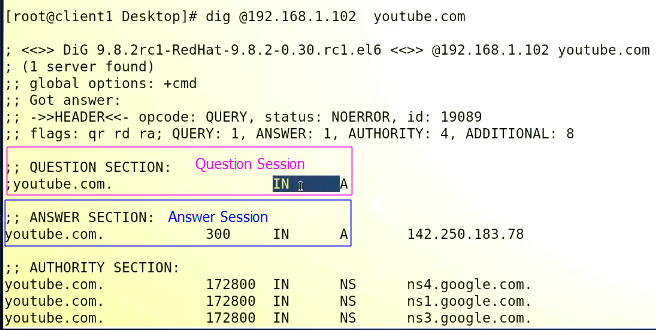
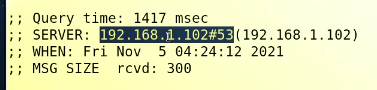
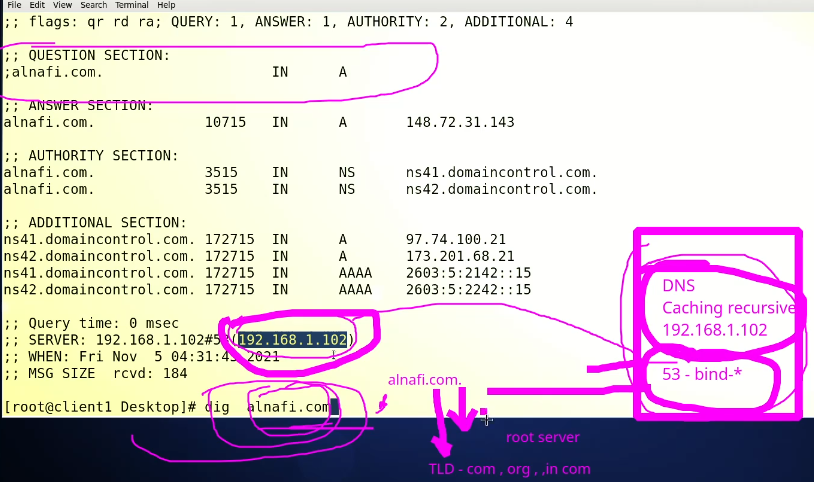
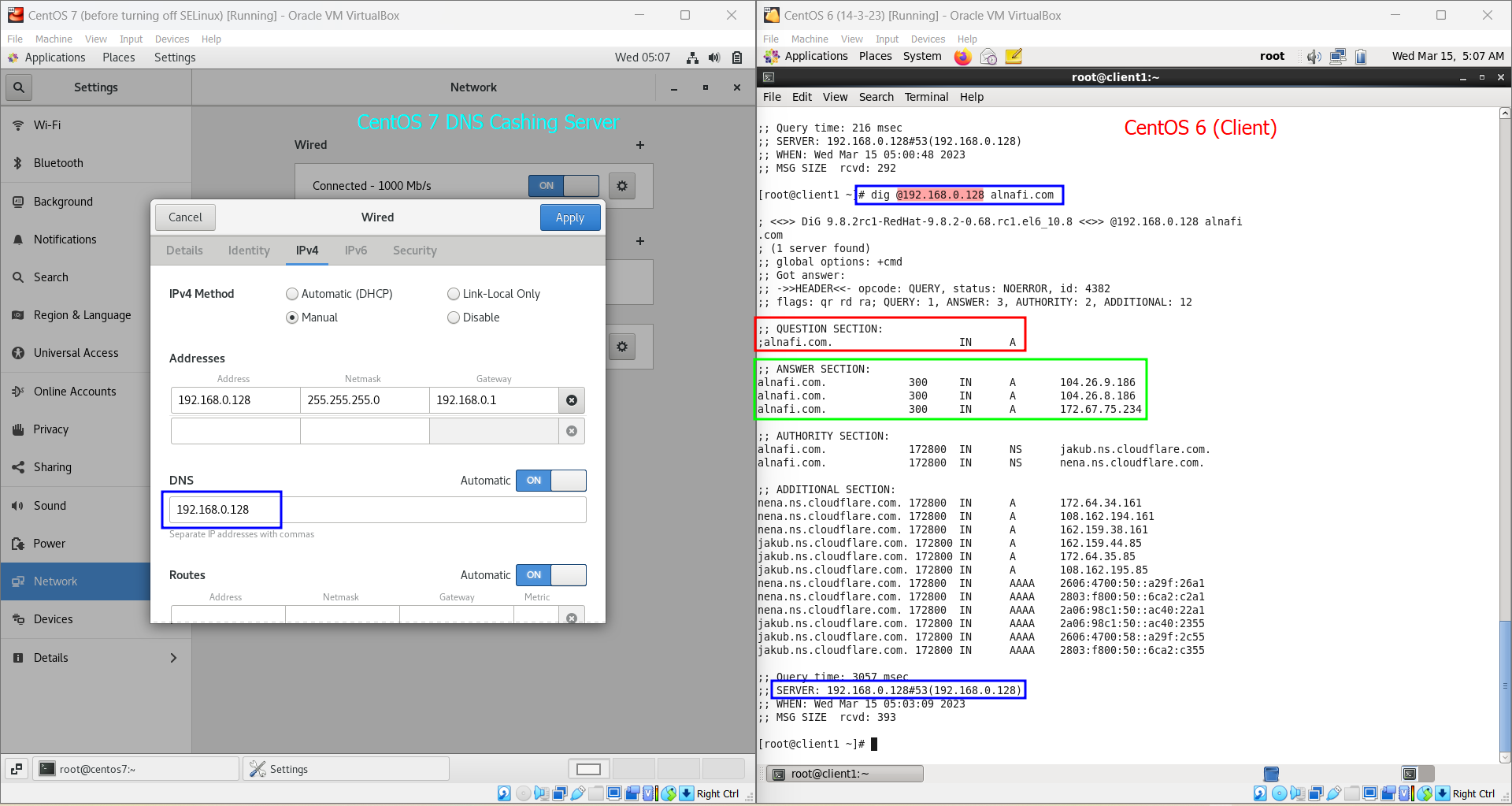
* Required package 🡪**”bind-\*”**
* **$ yum install bind-\* -y**
* 
* If we don’t have our own DNS server, the clients on a private network will go to the internet for DNS btu if we created our own DNS, then our server will do the job and clients in the private network will remain inside the network.
* Install bind package
* Root directory of DNS 🡪 **/var/namd/chroot**
* cd /var
* We need to move “named.conf” file in /etc to /opt
* while setting up DNS caching server, is it mandatory to move *"named.conf"* file to other location?
* No, it is not mandatory to move the *"named.conf"* file to another location while setting up a DNS caching server. The *"named.conf"* file is the configuration file for the BIND DNS server, and it specifies the settings for the server, including zone information, access controls, and logging information.
* *However, some administrators prefer to move the "named.conf" file to another location to improve security. By default, the "named.conf" file is usually located in the "/etc/named" directory, which may be accessible to other users on the system. Moving the "named.conf" file to a different location, such as a restricted directory, can help prevent unauthorized access to the configuration file.*
* If you choose to move the "named.conf" file, be sure to update the configuration settings to point to the new location of the file.

But Sir Kazim explained “we do not need it here, actually we need the file insiden “/var/named/chroot”.

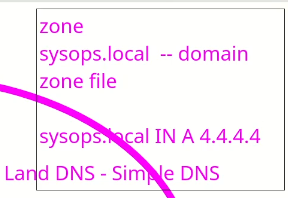
* 
* Now start the service 🡪 $ systemctl start named-chroot
* To verify is service is running,
* 
* To check if post No, 53 is up,
* 
* How to open / ad port in firewall
* **$ firewall-cmd --permanent --add-service=dns**
* 
* Service is added in firewall 🡪 (I restarted the firewall to get the service listed in it)
* =============================================

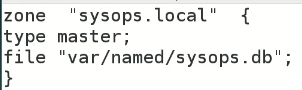
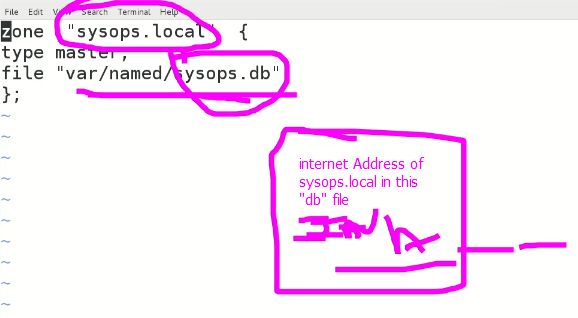
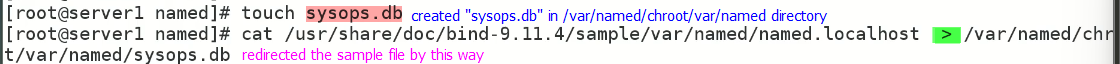
At this point “Cashing Recursive **DNS Service** is configured successfully.

Go to client, edit /etc/resolv.conf and add, 🡪 without this step DNS Servdr will not work properly.

* nameserver <DNS server IP Add)>
* $ dig @192.168.1.102 youtube.com 🡪 to get youtube Public IP address 🡪 it is called “**txt query” or TXT lookup**
* This query uses TCP or UDP protocols.
* **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol) are both transport layer protocols that are used to establish communication between two devices over a network.
* TCP is a connection-oriented protocol, which means that a connection must be established between two devices before data can be exchanged. TCP provides reliable, ordered, and error-checked delivery of data between applications running on devices. This is achieved by using acknowledgments and retransmission of lost or corrupted packets. TCP is commonly used for applications such as file transfer, email, and web browsing.
* UDP, on the other hand, is a connectionless protocol, which means that data can be sent without establishing a connection first. UDP does not provide any guarantees of reliable or ordered delivery of data, and there are no acknowledgments or retransmissions of lost or corrupted packets. UDP is commonly used for applications such as online gaming, video streaming, and VoIP (voice over IP) because it requires less overhead and can provide faster delivery of data than TCP.
* In summary, TCP provides reliable and ordered delivery of data at the cost of increased overhead, while UDP provides faster delivery of data with no guarantees of reliability or order. The choice of which protocol to use depends on the specific needs of the application being used.
  + nameserver 192.168.0.128 (IP address of DNS Cashing Server) and save it.
* . 
  + It is called “A record”.
* 
* how “dig” query works.
* 
* Initially I was not able to configure the DNS Cashing Server but I fixed as shown below,
* I edited network Interface on DNS Server (CentOS 7) and changed DNS setting by IP address of CentOS 7.
* The DNS Cashing Server is resolving requests from CentOS 6 (client).
* 

**Land DNS Server**

* Simple DNS
* It doesn’t access internet.
* It resolves requests locally.
  + We need to create “zone” or “forward zone”.
  + 
* Text

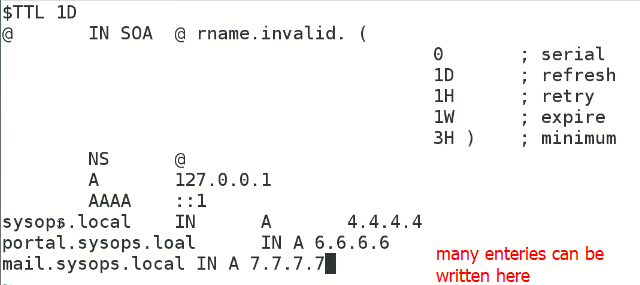
  Description automatically generated
* Go to ../chroot/etc
* Edit ***“named.conf****”* file.
* 
* We will write Internet Address of “sysops.local” in “**sysops.db**” file as mentioned in this file.
* The path “/var/named/sysops.db” means its home directory understandably is ***/var/named/chroot.***
* 
* Now go to this location 🡪 ***/var/named/chroot/var/named/***
* And create “sysops.db” file.
* Since, we don’t know how to edit it, we will use this path
* 
* To copy a sample file to /var/named/chroot/var/named/ directory.
* (we did similarly while configuring “httpd” (Apache) server)
* Sir Kazim redirected this sample file to “sysops.db”
* 
* If we open this file it contents looks like this,
* Graphical user interface, text, application

  Description automatically generated with medium confidence
* It is called zone file.
* $ vi sysops.db 🡪 to edit this file

Sir Kazim, *created this file in /var/named*

* Graphical user interface, text

  Description automatically generated
* .
* Graphical user interface, application, table

  Description automatically generated
* “@” is asking for origin and origin is “sysops.local”
* .
* 
* .
* Text, letter

  Description automatically generated
* **$ systemctl restart named-chroot**
* Now try ,
* $ dig @192.168.1.102 sysops.local
* This query should be resolved if the DNS Server is configured successfully.
* .

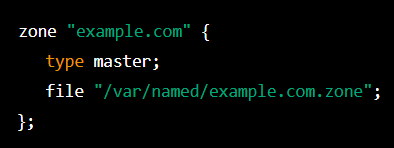
**how to create DNS land server or simple server using CentOS 7?**

Here are the steps to create a DNS server using CentOS 7:

1. Install BIND: BIND (Berkeley Internet Name Domain) is a popular DNS server software. To install BIND on CentOS 7, run the following command:



1. Configure BIND: The configuration file for BIND is located at **/etc/named.conf**. Open the file in a text editor and add your DNS zones to the file. Here is an example zone configuration for a domain called example.com:



1. Create the zone file: Create a new file called **/var/named/example.com.zone** (replace example.com with your domain name) and add the necessary DNS records for your domain. Here is an example zone file for example.com:

Text

Description automatically generated

This is an example zone file for a DNS server that is hosting the **example.com** domain. Here is a breakdown of the file:

* **$TTL 86400**: Sets the time-to-live (TTL) value for the zone file to 86400 seconds (1 day).
* **@ IN SOA ns1.example.com. admin.example.com. ( ... )**: Specifies the start of authority (SOA) record for the zone. The **@** symbol is a shorthand for the zone name (**example.com**). The **NS** records for this zone point to **ns1.example.com** and **ns2.example.com**. The **SOA** record specifies the primary DNS server for the zone (**ns1.example.com**), the email address of the zone administrator (**admin.example.com**), and several other parameters.
* **@ IN NS ns1.example.com.**: Specifies that **ns1.example.com** is a name server for the zone.
* **@ IN NS ns2.example.com.**: Specifies that **ns2.example.com** is a name server for the zone.
* **ns1 IN A 192.168.1.10**: Specifies that the IP address of **ns1.example.com** is **192.168.1.10**.
* **ns2 IN A 192.168.1.11**: Specifies that the IP address of **ns2.example.com** is **192.168.1.11**.
* **www IN A 192.168.1.12**: Specifies that the IP address of **www.example.com** is **192.168.1.12**.

This zone file defines the DNS records for the **example.com** domain, including the name servers for the domain (**ns1.example.com** and **ns2.example.com**) and the IP address of the web server (**www.example.com**).

1. Start BIND: Start the BIND service by running the following command:



1. Configure firewall: If you have a firewall enabled on your CentOS 7 server, you need to allow DNS traffic through the firewall. To do this, run the following commands:

Text

Description automatically generated with medium confidence

That's it! Your DNS server is now up and running. You can test it by pointing a domain's DNS records to your server's IP address and checking that the DNS records resolve correctly.