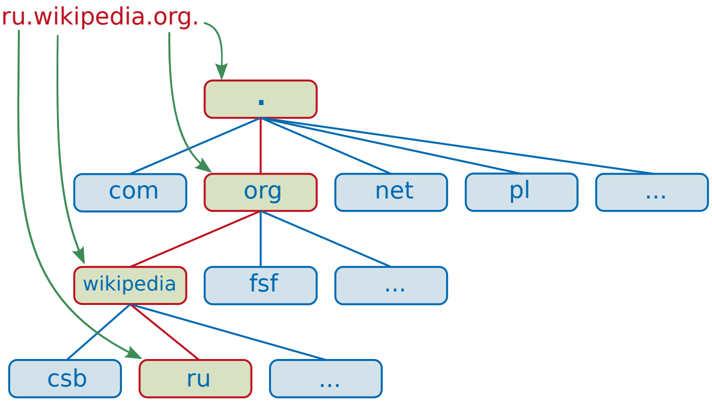
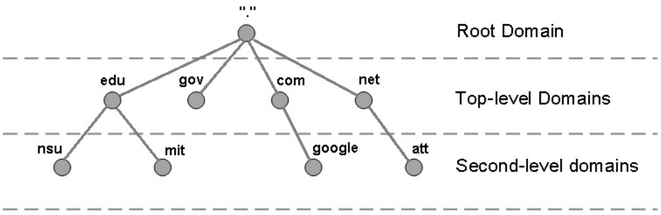
DNS

DNS is composed of a hierarchical domain name space





The DNS root zone is the top-level DNS zone in the hierarchical namespace of the Domain Name System (DNS) of the Internet.

How many Root name servers exist in the public DNS hierarchy?
13

Top-level domain (TLD)
refers to the last segment of a domain name, or the part that follows immediately after the "dot" symbol. TLDs are mainly classified into two categories: generic TLDs and country-specific TLDs. Examples of some of the popular TLDs include .com, .org, .net, .gov, .biz and .edu.

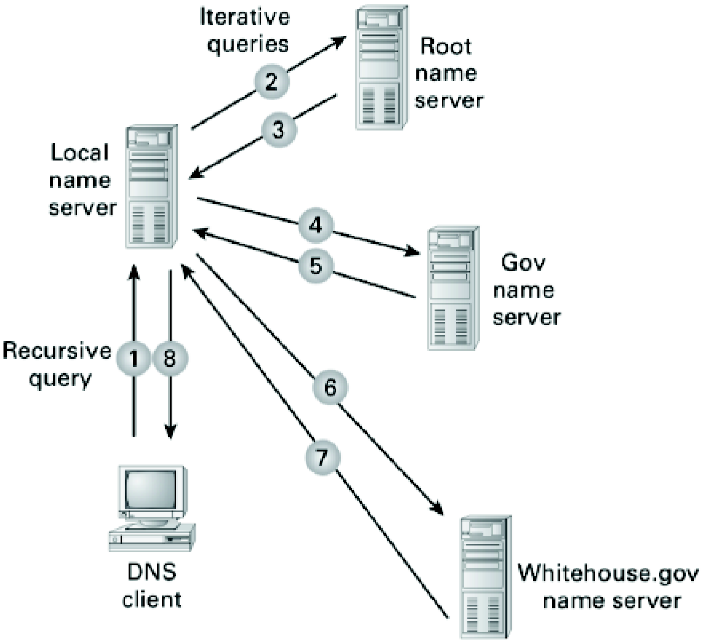
A fully qualified domain name (FQDN), sometimes also referred to as an absolute domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including at least a second-level domain and a top-level domain.

The DNS root domain is unnamed which is expressed by having an empty label in the DNS hierarchy, resulting in a fully qualified domain name ending with the top-level domain. However, in some cases the full stop (period (the dot at the end)) character is required at the end of the fully qualified domain name. It is the same to write:
www.google.com
www.google.com.

In contrast to a domain name that is fully specified, a domain name that does not include the full path of labels up to the DNS root is often called a partially qualified domain name.

What typical transport layer protocol and port does DNS use for DNS lookups?
UDP (User Datagram Protocol)
Con respecto al port, con el WireShark en mi computadora:
Source prot: 42440
Destination port: 53

Here’s what happens to resolve the request (DNS Resolution):
0. The resolver first check two places in its memory.
 * Its cache memory: ipconfig /displaydns
 * The host text file.
 * if there is no record in either of these files:
1. The resolver sends a **recursive DNS query** to its local DNS server asking for the IP address of www.whitehouse.gov. The local name server is responsible for resolving the name.
2. The local name server checks its zones, and it finds no zones corresponding to the requested domain name:
 * Because is a recursive DNS query, the local DNS server replay to the resolver: "I don't know.. but I will find it for you.. It is my job"
 * So it will start an Iterative query with other DNS server
3. The local DNS server sends an Iterative query to . root name server domain. The root name server has authority for the root domain, and it will reply with the IP address of a name server for the .gov top-level domain.
4. The local name server sends an iterative query for www.whitehouse.gov to the Gov name server.
5. The Gov name server replies with the IP address of the name server servicing the whitehouse.gov domain.
6. The local name server sends an iterative query for www.whitehouse.gov to the whitehouse.gov name server.
7. The whitehouse.gov name server replies with the IP address corresponding to www.whitehouse.gov
8. The local name server sends the IP address of www.whitehouse.gov back to the original resolver.



Recursive Queries
- Recursive queries are between the client and its local DNS server
- In a recursive query, the client sends a query to its local DNS server asking it to respond either with the requested answer or with an error message. The error states one of two things:
 * The local DNS server doesn't know the answer:
  ~ In this case start an Iterative queries with other DNS server
 * The domain name doesn’t exist.
- As we can see, in a recursive query, the name server isn't allowed just to refer the client to some other name server. It have to respond to the client.
- In addition, if your DNS server uses a forwarder, the requests sent by your server to the forwarder will be recursive queries.

Iterative Queries
- Iterative queries are between the local DNS server and other DNS servers. During the iterative queris, the other DNS servers can simply provide a referral if they don't know the requested IP address.

What is a DNS forwarder
A forwarder is a Domain Name System (DNS) server on a network used to forward DNS queries to DNS servers outside of that network.

If no DNS server is designated as the forwarder to which external queries are routed, then all DNS servers within the network will handle external requests, which means that they will query external resolvers. This is undesirable for two main reasons:

1 - **Internal DNS information can be exposed on the open Internet.** It's far better to have a strict separation between internal and external DNS. **Exposing internal domains on the open Internet creates a potential security and privacy vulnerability.**

2 **Without forwarding, all DNS servers will query external DNS resolvers if they don't have the required addresses cached. This can result in excessive network traffic. By designating a DNS server as a forwarder, that server is responsible for all external DNS resolution and can build up a cache of external addresses, reducing the need to query recursive resolvers and cutting down on traffic.** For smaller companies with limited available bandwidth, DNS forwarding can increase the efficiency of the network by both reducing bandwidth usage and improving the speed at which DNS requests are fulfilled.

DNS zone

- **A DNS zone** is a portion of the DNS namespace over which a specific DNS server has authority.
- Within a given DNS zone, there are resource records (RRs) that define the hosts and other types of information that make up the database for the zone.

- **DNS Zone Types:** We have two different types:
  * **The most common type is a forward lookup zone**
    ~ Everybody knows this is how DNS works. The point to a forward lookup zone is that you have a computer name or a host name, and you'd like to get the IP address for that. So, host name to IP address resolutUDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.ion, that's a forward lookup.
    ~ Forward lookup zones contain **authoritative data.** Authoritative data means that the data lives on the server where the client got the DNS response from. **Non-authoritative** answers were when the DNS server that the client asked the query of had to go out and find it someplace else, and then that DNS server would put it in its cache.
  * **Reverse lookup zones:** The purpose here is that you have the IP address and you need to get a resolution to the host name, so you're going the opposite direction.
    ~ The command **traceroute**, for example, is related with reverse lookup zones

- Zone files consist of a number of resource records
There are different types of resource records that could be placed in a forward lookup zone:
  * One of the most common resource records out there are a **host record. An A record is an IPv4 host record.**
  * **An AAAA**, well, that's an IPv6 host record
  * **PTR**, or pointer records, are the records that reside in a reverse lookup zone that point to the host record in the forward lookup zone.
  * **A CName**, or canonical name, is really a nickname of a machine. So if you have a server in your environment, and you'd like for people to access it using different names for whatever reason, you can set up CName records to point to a host record.
  * **An SRV record**, or service locator record, denotes different types of services running on a machine. For example, in a Microsoft environment, if a client machine wanted to find a domain controller, it would send a query to a DNS server asking for the SRV records for the domain, and then it would get a list of domain controllers or DCs that it could authenticate against for whatever purpose the user is doing.
  * **MX records.** These are mail exchange records, and they denote a mail server. In a Microsoft environment, it would be an exchange server.

UDP (User Datagram Protocol)

UDP provides no guarantees to the upper layer protocol for message delivery and the UDP layer retains no state of UDP messages once sent. For this reason, UDP sometimes is referred to as Unreliable Datagram Protocol.
UDP is connectionless and does not require a session setup as does TCP. DNS, for example, use UDP protocol. DNS queries and responses are very small and do not require the overhead of TCP.

Comandos

nslookup
Stands for name server lookup. It's used to obtain domain name or IP address mapping or for any other specific DNS record:
$ nslookup sinfronteras.ws

netstat
Stands for network statistics; IT's a command-line network utility tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics
$ netstat -an | more
Con el comando anterior se puede ver where is your machine connecting to.

DHCP

- Is it required on every IP network?

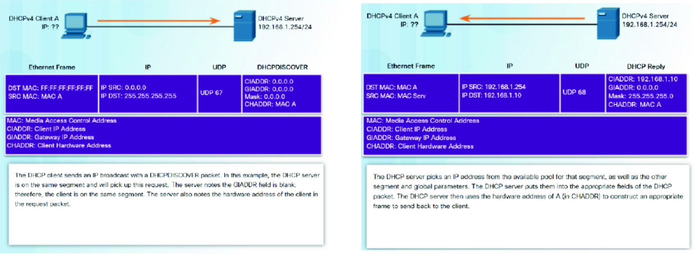
Understanging DHCP address assignment
What is the four step process to retrieve IP configuration information?
Use a labelled diagram to show this.
Four step process for a client to obtain a lease:
Broadcast DHCP Discovery (DHCPDISCOVER): The client Broadcasts a DHCP Discovery message (Layer 2 and Layer 3 broadcast) to the local network to identify any available DHCP servers. This broadcast reaches only as far as the nearest router.

Respond with DHCP offer (DHCPOFFER): If a DHCP server is connected to the local network, it unicast a DHCP offer messaget for the DHCP client (binding DHCPOFFER message as unicast). The DHCP message contains a list of DHCP configuration parameters and an available IP addresss form the DHCP scope. If the DHCP server has an IP address reservation that matches the DHCP client's MAC address, it offers the reserved IP address to the DHCP client.

Respond with DHCP request (DHCPREQUEST): The client responds to the DHCP message and requests the IP address contained in this DHCP offer message. Alternatively, the client might request the IP address that was previously assigned.

Confirm with DHCP Ack (DHCPACK): If the IP address request by the client is still available, the DHCP server responds with a DHCP Ack (acknowledgement) message (unicast DHCPACK message). The client can now use the IP address.

DHCPv4 Operation
DHCPv4 Discover and Offer Messages



The DHCP client sends an IP broadcast with a DHCPDISCOVER packet. In this example, the DHCP server is on the same segment and will pick up this request. The server notes the GIADDR field is blank; therefore, the client is on the same segment. The server also notes the hardware address of the client in the request packet.

The DHCP server picks an IP address from the available pool for that segment, as well as the other segment and global parameters. The DHCP server puts them into the appropriate fields of the DHCP packet. The DHCP server then uses the hardware address of A (in CHADDR) to construct an appropriate frame to send back to the client.

De la figura anterior se debe notar que el client en el discovery message contiene DST MAC: FF.FF.FF.FF.FF.FF. El client no conoce en ese momento la DST MAC (es un broadcast) que se hace precisamente para saber quien es el DHCP server. Me imagino entonces que es uan addresss que se coloca por defecto y podría tener la función de identificar el paquete como lo que es, un DHCP discovery message.

Also notice that The GIADDR field in relayed DHCP packets identifies the relaying gateway. The DHCP server uses the GIADDR to select an IP address pool (also known as the DHCP scope) from which to assign the IP addresses. Return packets from the DHCP server are always sent to the GIADDR. Lo que entiendo de de la explicación que se muestra en la figura es que: "este campo está en blanco, lo que significa que el

paquete no ha pasado por ninguna gateway y está por lo tanto en el mismo segment; therefor, el Server sabe que tiene que asignar una address de esa red. Lo que indica que el DHCP server puede estar proporsionando IP addresses en más de una red". Se tiende a pensar que el DHCP server tiene que estar en la misma red porque el discover message esun broadcast. Sin embargo, si se puede configurar un DNS que esté en otra red: On a Cisco Router, the ip helper-address command configures the device as a DHCP relay agent. The DHCP relay agent forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.
DHCP requests are broadcasts. Routers (Layer 3 devices) suppress broadcast traffic. So if the DHCP server resides in a remote network, a DHCP relay agent is required to handle the requests beyond the local subnet. En otras palabras: A Cisco IOS helper address is configured so that the router acts as a relay agent forwarding the message to the DHCPv4 server.

Algunos campos en el Discover and Offer Messages packet:
client IPv4 address (CIADDR)
default gateway address (GIADDR)

Option 1:	Subnet Mask
Option 3:	Router IP address
Option 6:	DNS IP addresss
Option 51	IP address lease time
Option 53:	DHCP Message type (Offer)
Option 150:	

A Cisco IOS helper address is configured so that the router acts as a relay agent forwarding the message to the DHCPv4 server

DHCPv4 messages:
- If sent from the client, use UDP source port 68 and destination port 67.
- If sent from the server, use UDP source port 67 and destination port 68.

ARP: Address Resolution Protocole - layer 2 (data link later)
It's a protocol used to match an IP address with its corresponding MAC address on a LAN. The MAC address is required to send packets within a LAN.
ARP broadcast: An ARP broadcast is sent to a broadcast Ethernet address, so everyone on the LAN receives
ARP cache: a record of IP addresses and MAC addresses.
How ARP works: https://www.youtube.com/watch?v=1jncvd6JDoc
Step 1: Check the ARP cache: To verify if there is already an MAC address corresponding with the IP address in question.
Step 2: Generate an ARP request message: This massage include the IP and MAC address of the source device and the IP address of the destination device. Of course, it doesn't include the MAC address of the destination device because that is what it is looking for.
Step 3: Send the ARP request as a Broadcast message.
Step 4: All local devices process the ARP request message. Only one device will realize the ARP request message contain its IP address. This device will reply this ARP request message. The rest of devices will discard the message.
Step 5: The corresponding destination device generate the ARP reply message. This ARP reply message include add the MAC address of the destination device to the ARP request message. So this massage include the IP and MAC addresses of the Source an Destination devices.
Step 6: The destination device update its ARP cache since it now knows the IP and MAC address of the source device.
Step 7: The destination device sends the ARP reply message (unicast) back to the source device.
Step 8. The source device update its ARP cache: The source device processes the ARP reply message and Update its ARP cache to include the MAC address of the such destination device.

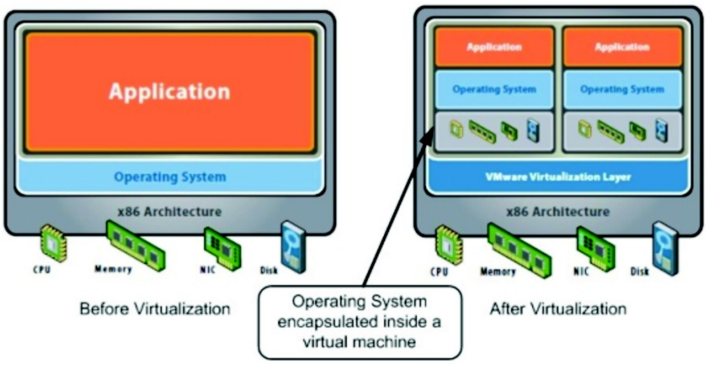
IP Address: a device address that allows devices to transport packets from network to network via Routers. An IP address can not be used to transmit data within a LAN.

MAC address: ia a unique physical address assigned and burned into a device network interface card (NIC). A MAC address allows a device to transmit data within a LAN.

Private IP Addresses:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

A hypervisor, also called virtual machine manager (VMM), is one of many hardware virtualization techniques allowing multiple operating systems, termed guests, to run concurrently on a host computer.
There are two types of Hypervisor:
- **Type 1 (Bare Metal Hypervisor):** A Type 1 hypervisor, also known as a **bare metal hypervisor**, is software installed directly onto a physical computer.
  * E.G VMware use a hypervisor called ESXi

- **Type 2 (Hosted Hypervisor):** A Type 2 hypervisor provides hypervisor functionality above, or on top of an already installed operating system. In short, the hypervisor is installed as an application, providing the platform for VMs. An example would be Oracle Virtualbox running on Windows 10 PC.



Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

What is the difference between an authoritative versus a authoritative response?

Which of the following is a Layer 2 Broadcast Address used by DHCP? Select all of the correct answer(s).
i. 1111.1111.1111
ii. ffff.ffff.ffff
iii. 255.255.255.255
iv. 0000.0000.0000

Practicar Wireshark:
- Use Wireshark to view ARP messages
- Utilize Wireshark to see if your VM is using your DNS forwarder
- Pag 4 - Revision part 2

<u>DHCP configuration on Cisco routers:</u>
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
Specifies the range of addresses not to be leased out to clients.

Router(config)#ip dhcp pool CCT
Creates a DHCP pool named in this case CCT. The name can be anything of your choosing.

Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Defines the range of addresses to be leased.

Router(dhcp-config)#default-router 192.168.0.1
Defines the address of the default router for the client.

Router(dhcp-config)#dns-server 8.8.8.8
Defines the address of the Domain Name Server for the client

Verify DHCPv4 configuration using the show running-config | section dhcp command

Verify the operation of DHCPv4 using the show ip dhcp binding

Configure dynamic, default, and static routing on the routers.

Configure RIPv2 for R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.252
R1(config-router)# no auto-summary
```

Configure RIPv2 and a default route to the ISP on R2.

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 192.168.2.252
R2(config-router)# default-information originate
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

The above configuration in b) firstly sets up rip version 2 for the network 192.168.2.0. Then using the line default-information originate command, it tells the router if the IPv4 routing table has a default route in it, advertise a default route with RIP.

IOS allows the configuration of a static default route by using special values for the subnet and mask fields in the ip route command: 0.0.0.0 0.0.0.0. For example the command ip route 0.0.0.0 0.0.0.0 209.165.200.225 creates a static default route on R2 – a route that matches all IP packets and sends those packets out to the next hop of the ISP router.

Configure a summary static route on ISP to reach the networks on the R1 and R2 routers

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```