Networking and Internet Services

Presented by
Omid panahi

Goals of this section

- Install and configure DNS
- Analyze and interpret the output of troubleshooting tools: command line tools (ipconfig, netstat, ping, tracert, nslookup)
- Compare and contrast the following ports and protocols: NetBIOS
- Given a scenario, configure and apply the appropriate ports and protocols: DNS, SMB

Introduction

- Although computers use IP addresses to communicate with each other over a TCP/IP network, people prefer easy-to-remember names over IP addresses.
- It's easier to remember SRV-LAN-NAS01 rather than 172.20.20.20!
- We can't expect everyone to be technical and remember IP addresses all the time.

Name Resolution

- Converts IPv4 addresses to names, and names to IPv4.
- (Also IPv6)
- The protocol is formally called "Domain Name Resolution" or "DNS" in short for "Domain Name System".
- Where is DNS present?
- At home, on your lan. (Examples?)
- At work for the domain.
- On the Internet as a whole.

Before DNS

- System called NetBIOS was used
- Used broadcasts for name resolution
- When a computer booted up, it broadcast its name along with its MAC address
- Every other NetBIOS system heard the message and stored the information in a cache
- Used for SMALL networks
- Used to share files and printers

Modern NetBIOS

- NetBIOS is still alive under the name "*NetBIOS over TCP/IP (NetBT)" which* runs NetBIOS on top of TCP/IP.

-

Try This!

Checking Out NetBIOS

Grab a handy Windows or Linux system and try running **netstat -a -n**. Can you find open or listening ports on port numbers 137, 138, 139, and 445? If you have a Windows system, you will see these. Systems listening on those ports show NetBT and SMB running just fine.

Get the name from the IP address

- Most of the time, we can get the machine network name via the PING command.

```
C:\Users\opanahi>ping -a 172.26.128.1

Pinging SLB-CSCI-OMIDPL.mshome.net [172.26.128.1] with 32 bytes of data:
Reply from 172.26.128.1: bytes=32 time<1ms TTL=128
Reply from 172.26.128.1: bytes=32 time<1ms TTL=128
Reply from 172.26.128.1: bytes=32 time<1ms TTL=128
Reply from 172.26.128.1: bytes=32 time<1ms TTL=128
```

Host File

- A file that maps name to IP address.
- Used for overrides.
- In windows you can find it under
  C:\Windows\System32\Drivers\etc\

In linux → /etc/hosts

Example


```
PS C:\> cd .\Windows\System32\drivers\etc\
PS C:\Windows\System32\drivers\etc> ls


    Directory: C:\Windows\System32\drivers\etc


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/22/2025     2:08 AM           1050 hosts
-a----         10/23/2025     8:49 AM            444 hosts.ics
-a----          4/1/2024     3:24 AM           3683 lmhosts.sam
-a----          5/7/2022     1:22 AM            407 networks
-a----          5/7/2022     1:22 AM           1358 protocol
-a----          5/7/2022     1:22 AM          17635 services
```

192.168.2.1   server1
201.32.16.4   server2
12.22.23.11   www.example.com

Linux Host file (same concept)

```
127.0.0.1       localhost
127.0.1.1       SRV-LAN-L-01.brendan-wood.local SRV-LAN-L-01
```

Whats a good use for a host file?

- 1) SPAM FILTER!
  - ▫ http://winhelp2002.mvps.org/hosts.htm

- 2) Internal web sites.
  - ▫ 127.0.0.1   myfunnywebsite.com

- 3) Shortcuts
  - ▫ 23.33.168.88   steamstore
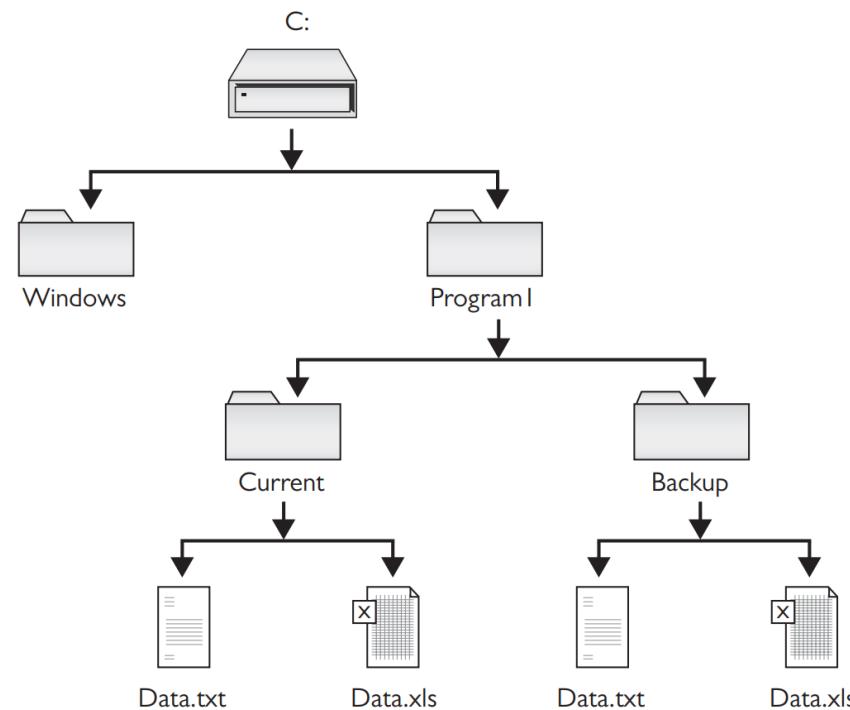
How DNS works

- DNS uses UDP port 53 (and TCP 53 also)
- The DNS root for the entire Internet consists of 13 powerful DNS server clusters scattered all over the world.
- http://www.root-servers.org/
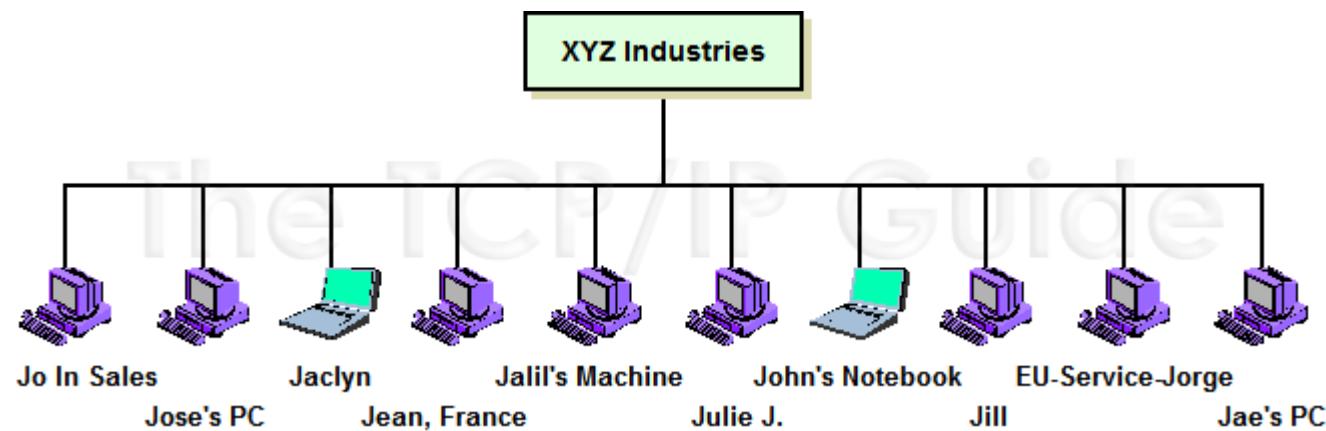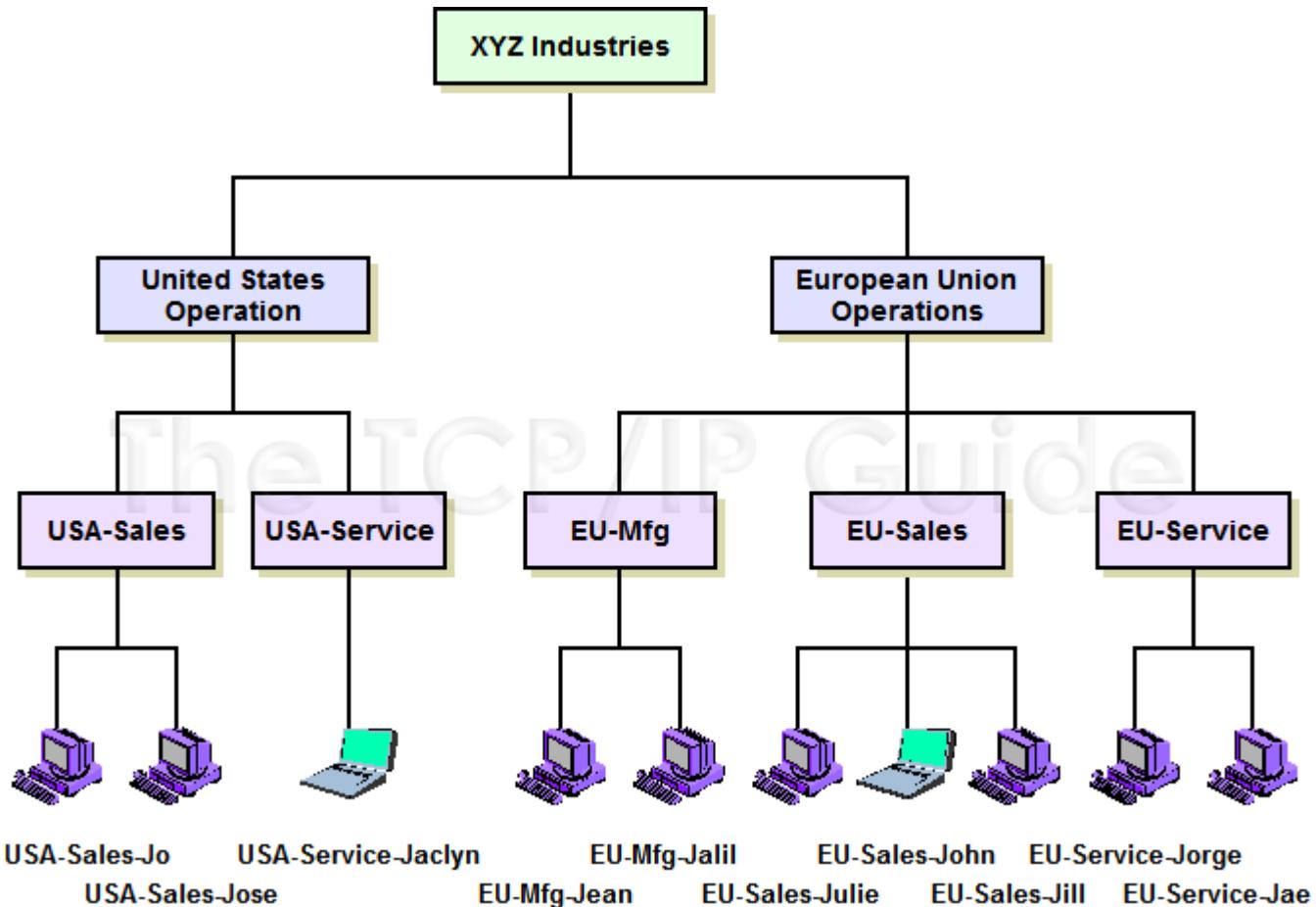
Name spaces

- What does hierarchical mean in terms of DNS? It is an imaginary tree structure of all possible names that could be used within a single system. By contrast, a hosts file uses a flat name space with no grouping whatsoever.
- In a flat name space, all names must be absolutely unique.

Directory terminology
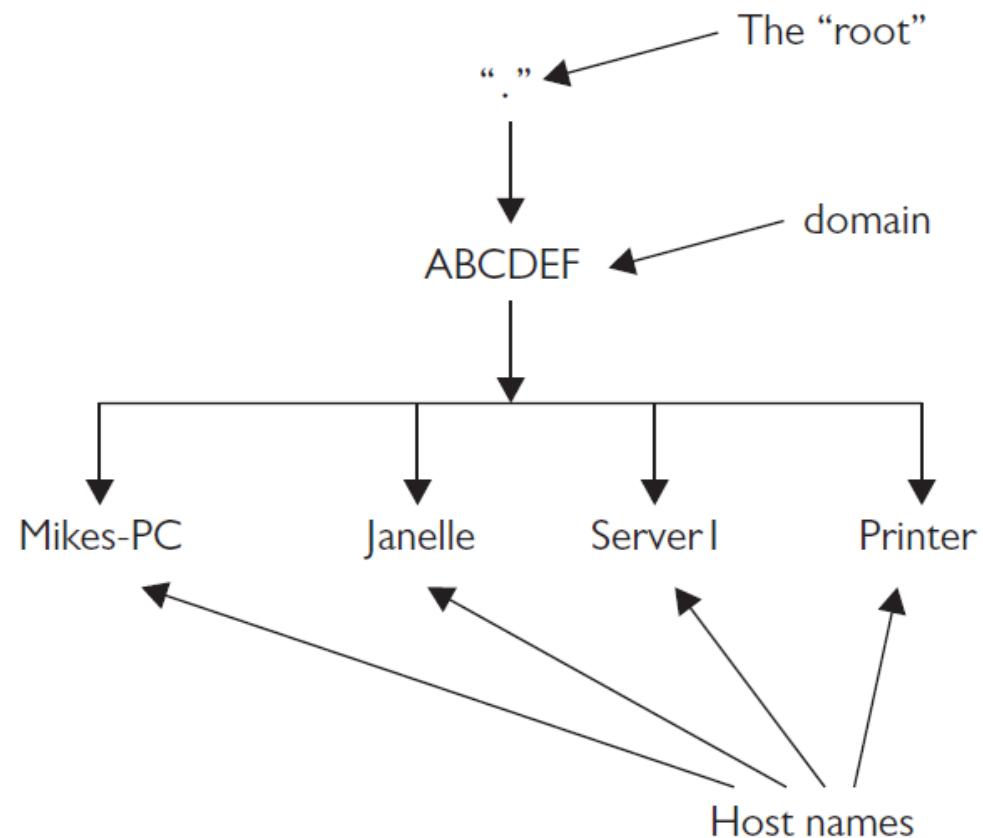
Flat VS Hierarchal Naming
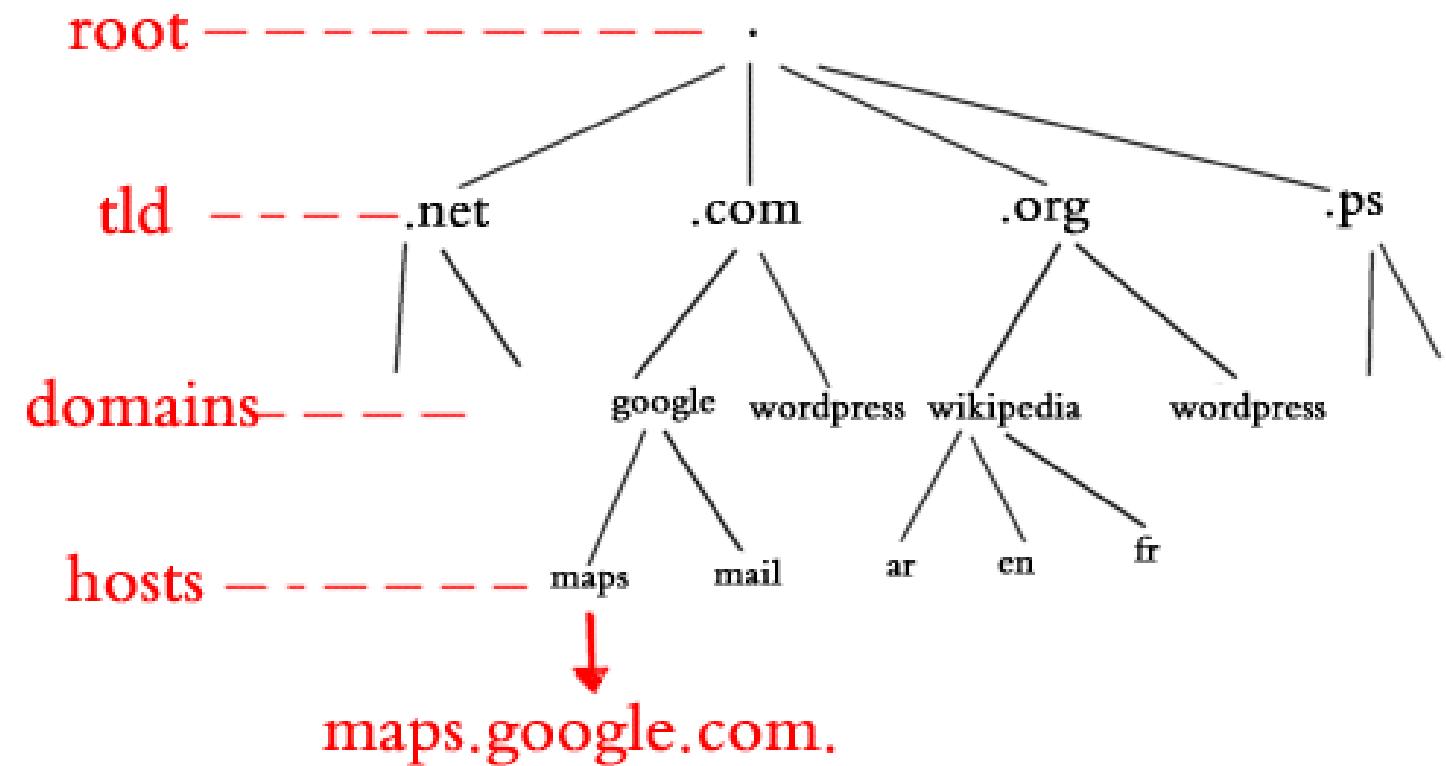
Private DNS tree

Heirarchy
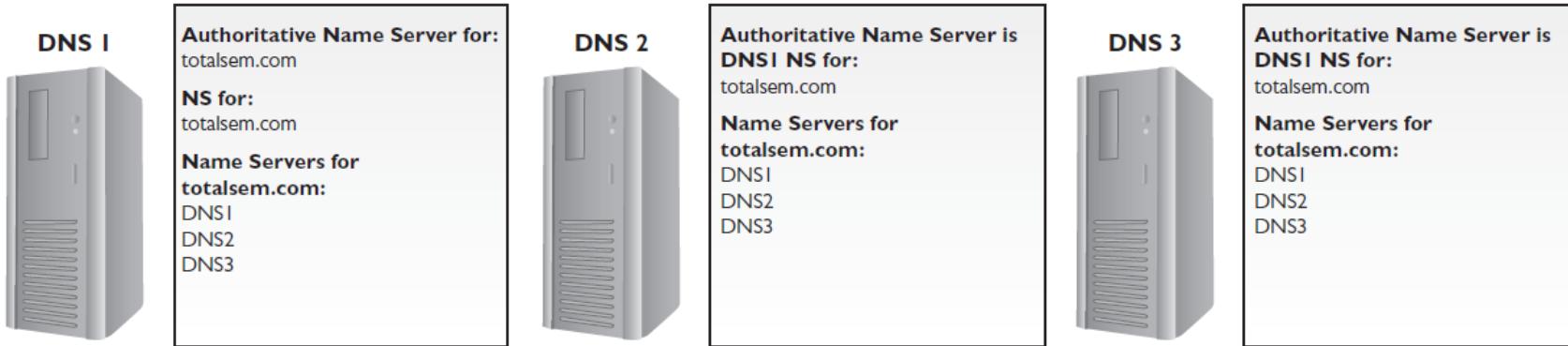
Name Servers
Definitions

- **DNS server** A *DNS server* is a computer running DNS server software.
- **Zone** A *zone* is a container for a single domain that gets filled with records.
- **Record** A *record* is a line in the zone data that maps an FQDN to an IP address.
- **Authoritative name server**: For a single domain, this DNS server holds ALL records. Eg: Microsoft.com

Child servers of the Auth-DNS server

DNS I

Authoritative Name Server for:
totalsem.com

NS for:
totalsem.com

Name Servers for totalsem.com:
DNS1
DNS2
DNS3

DNS 2

Authoritative Name Server is **DNSI NS for:**
totalsem.com

Name Servers for totalsem.com:
DNS1
DNS2
DNS3

DNS 3

Authoritative Name Server is **DNSI NS for:**
totalsem.com

**Name Servers for totalsem.com:**
DNS1
DNS2
DNS3
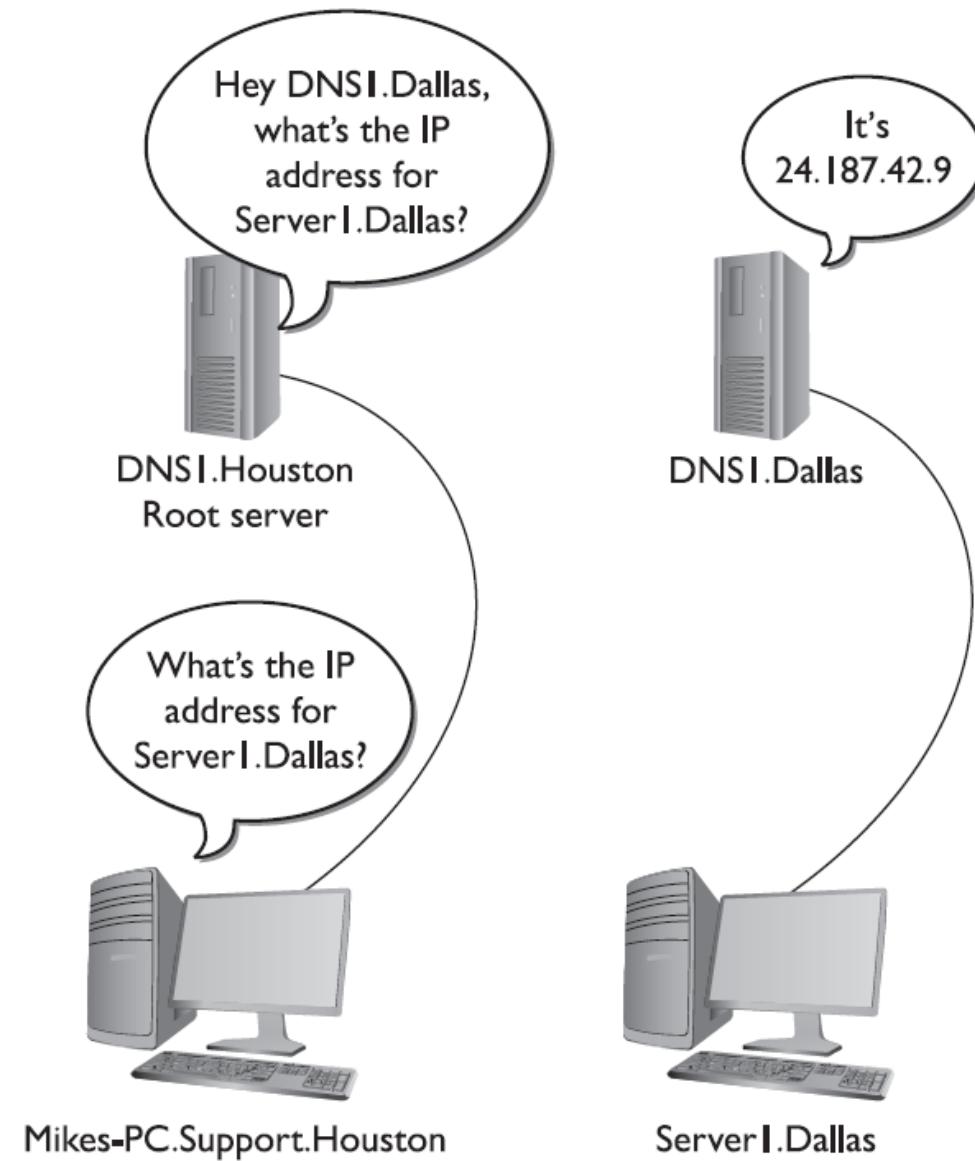
- Multiple DNS servers for the same domain must communicate frequently.
- When one DNS server receives a new record, it must propagate it to all others.
- Each DNS server knows:
    - ❑ The name and address of the **authoritative name server**.
    - ❑ The name and address of **every other DNS server** in the domain.

How it works

- Changes to the domain happen in the **authoritative** server.
- Then it propagates those changes downward to all the connected servers (see previous slide).
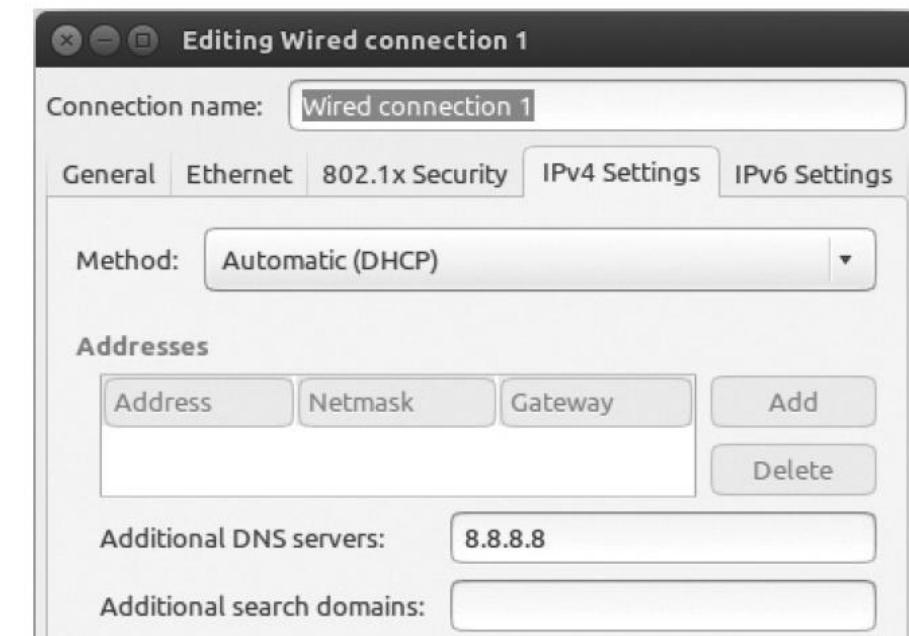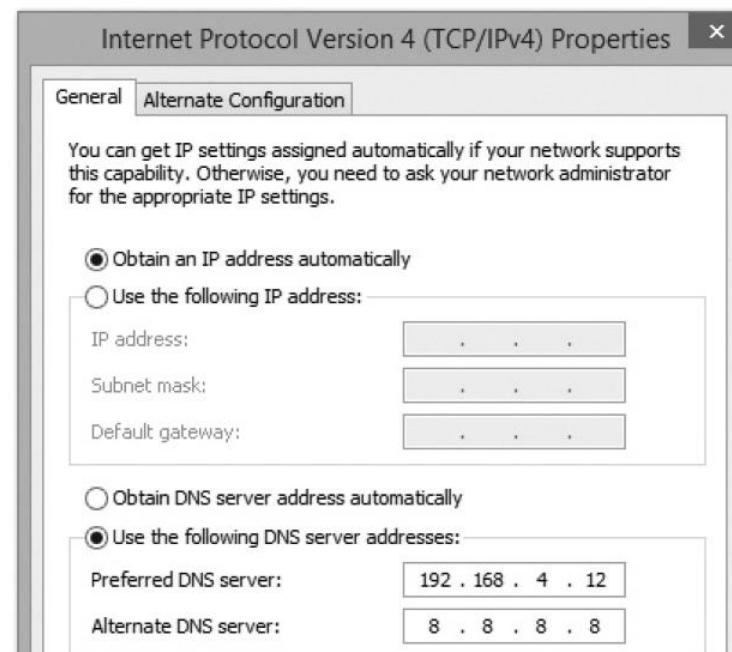
Root Servers

- Dns1.Houston = Root
- Dns1.Dallas = Child

- If a DNS query is not found in the root it searches the children DNS servers also.
- The reply is sent back up to the root and answered back to you.

DNS Server Settings

- Linux - /etc/resolv.conf
- Windows