
University of Colorado Boulder

Fundamentals of Data Communications

DHCP & DNS

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

Review

Dynamic Host Configuration Protocol (DHCP)

- **Every device needs an IP address**
  - Used to be manual on every machine
- **Dynamically assigns IP addresses**
  - IP address
  - Subnet mask
  - Default-gateway
  - Primary DNS server
  - Secondary DNS server
- **Server service**
  - Windows, Linux, Router
- **UDP**
  - Ports 67 & 68

Scope

- **Administrative grouping of range of addresses server can hand out**
- **10.1.1.100 - 10.1.1.200**
- **Keep static servers out of scope**
  - Reservations
  - Exclude Range
- **Host (hardware)**
- **Options**
  - DNS, Gateway, TFTP server, etc.

Lease

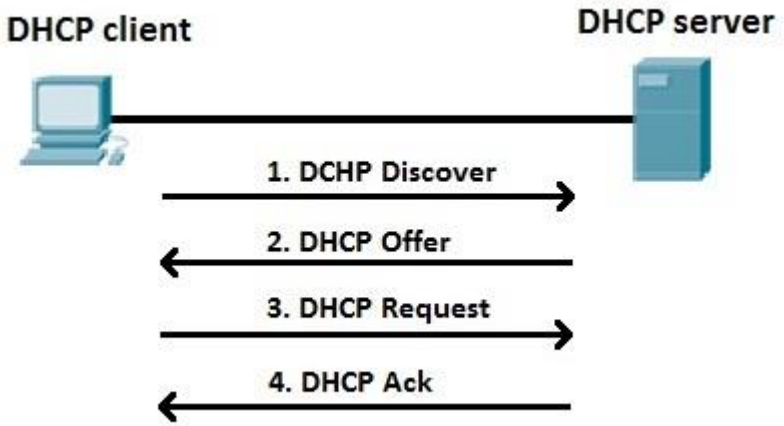
- **Limited number of addresses in the (pool/scope)**

- **1 day, 10 days, 100 days, etc.**
  - Coffee shop (1 day)
  - Large desktop enterprise (100 days)

- **50% of lease time; client requests to renew for another lease period**
  - Will re-try a random period of time (if can't contact server)
    - ***CSMA/CD***

DHCP – (DORA)

- **Client**
  - Discover Request – (Broadcast)
- **Server**
  - Offer
- **Client**
  - Request
- **Server**
  - Acknowledgement



Security

- **Multiple DHCP servers**
  - First response
- **What else?**

Notes

- **Misconfigure**
- **Multiple DHCP server**
- **Lease times**
- **Wireless Routers**
  - Rouge

Domain Name System (DNS)

Human Interaction

- **How do you call a business on the phone?**
  - You dial their phone number
  - You can't dial "Neptune Mountaineering"
- **How do you send someone postal mail?**
  - You label the postage with the address
- **How does this work for the Internet?**
  - I need to check my online checking account at Bank of America.
  - What is Bank of America's IP address?

Human Interaction

- **Computers use binary numbers (numerical IP addresses)**
  - IPv4: 173.252.110.27
  - IPv6: 2a03:2880:2110:df07:face:b00c:0:1
- **Humans typically can't remember multiple, long, arbitrary numbers**
- **Need a <u>system</u> to convert the numbers to a human-readable format**
  - Domain Name System (DNS)

Domain Name System (DNS) - Overview

- What is a **DOMAIN NAME**?
  - “Memorable,” “easy-to-spell” address that is unique on the Internet - (adtran.com vs. 76.164.174.122)

- What is an Uniform Resource Locator (URL)?
  - Domain name is part of a URL
  - Much more specific: folder, machine, protocol, etc.
  - adtran.com/support/tse_software

- DNS – The most recognized **<u>SYSTEM</u>** for assigning named addresses to hosts (Internet Web servers).

Remember!

- ***Domain Name System (DNS) is an international “phone book” for the Internet: it matches human-readable names to numbers (IP addresses) machines can understand.
  - Phone book/contacts maps phone number to name:
    - ***303-555-1000 = Levi Perigo***
  - DNS maps IP address to domain name:
    - ***128.138.183.242 = raveninnovation.com***

DNS - Understanding

- **What does DNS stand for?**
  - Domain Name System
- **What three pieces of information does a computer need to access the Internet?**
  - IP Address
  - Subnet Mask
  - Default Gateway
- **True or False: A computer must have a DNS server configured to access the Internet. Why or Why not?**
  - False. You can use the IP address of the server.
- **What are common DNS server IP addresses?**
  - 4.2.2.2 (Verizon)
  - 8.8.8.8 (Google)
  - 75.75.75.75 (Comcast)
  - 208.67.222.222 (OpenDNS)

History

- **Manual, centralized, 1:1 mapping system**
  - HOSTS.TXT
    - ***harvard.edu -> 69.172.200.24***
    - ***howard.edu -> 138.238.144.31***
    - ***howard.com -> 65.183.106.166***

- **This system failed**

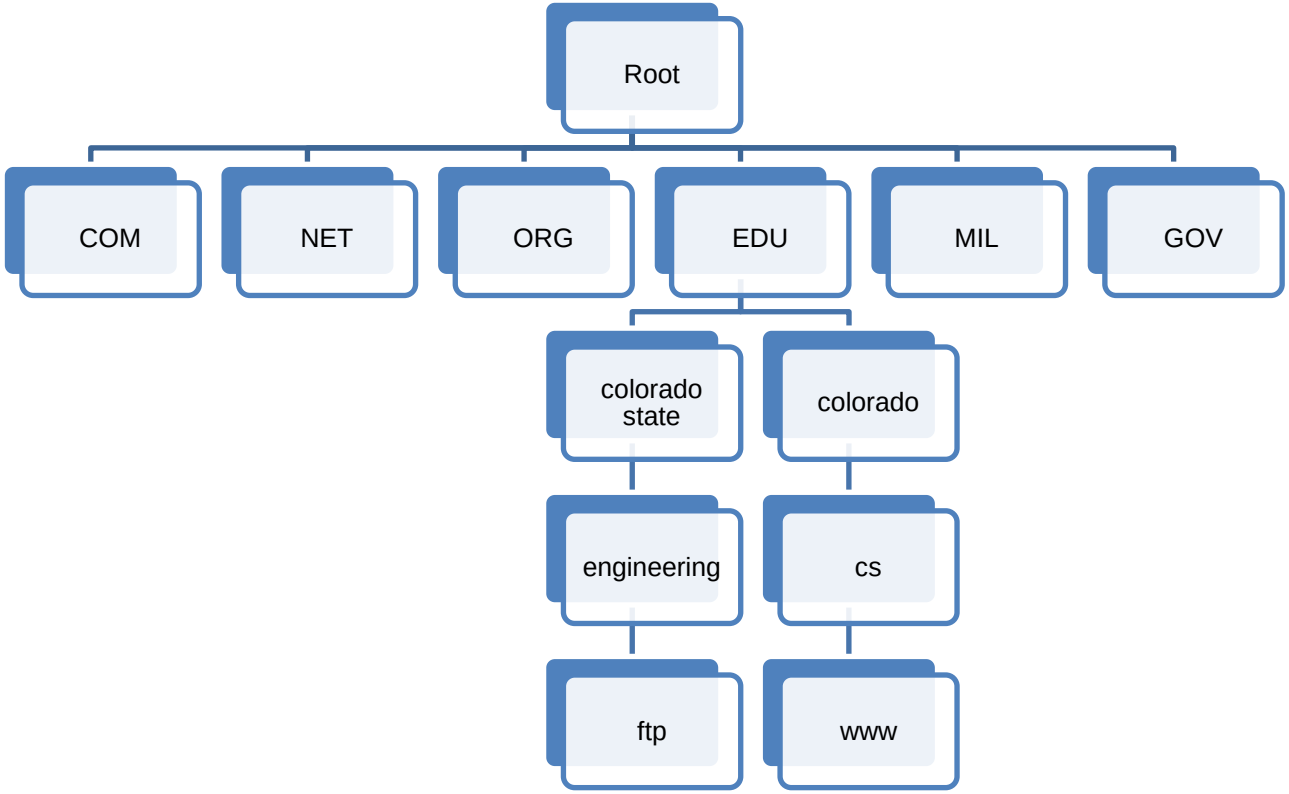
- **DNS – RFC 882 & 883 (1983)**

Design

- **Distributed Database**
  - Not centralized like “TEXT.TXT”
- **Client / Server**
  - UDP port 53 (some use TCP for large files)
- **DNS is a hierarchical tree structure**
  - .com -> google.com -> mail.google.com
- **Syntax**
  - 127 levels
  - 63 characters each
  - Max of 255 characters
  - LDH – letters, digits, hyphen; not case sensitive
  - Organized right to left
  - *Trivia – most US servers use three-letter TLDs (other countries often use two: .au; .ca; etc.)

Tree Structure

- **Top Level Domains (TLDs)**



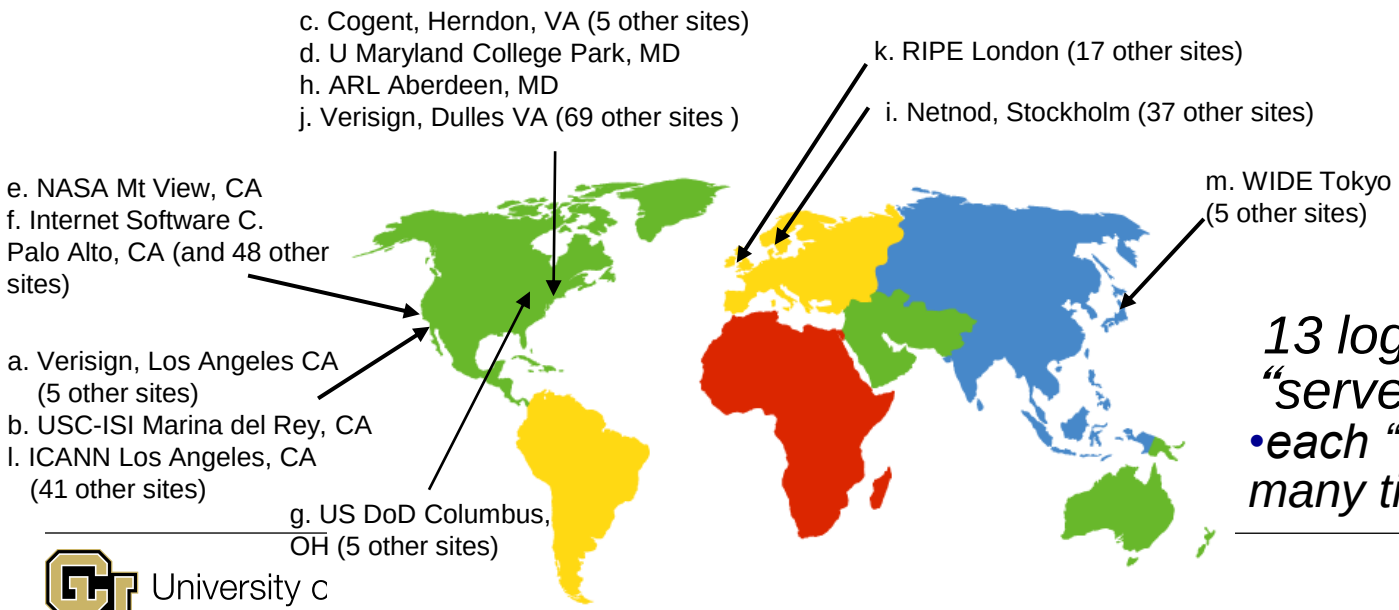
Tree Structure

- **Tree Zones**

- **Administration**
  - Internet Corporation for Assigned Names and Numbers (ICANN) - Root
  - VeriSign (gov; net)
  - Network Solutions (com)
  - Educause (edu)

DNS: root name servers

- **Contacted by local name server that can not resolve name**
- **Root name server:**
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server



13 logical root name "servers" worldwide

- *each "server" replicated many times*

TLD & Authoritative Servers

Top-level domain (TLD) servers:

- Responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
  - ***Network Solutions maintains servers for .com TLD***
  - ***Educause for .edu TLD***

Authoritative DNS servers:

- Organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
- Can be maintained by organization or service provider

Local DNS Name Server

- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one
  - also called "default name server"
- When host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

Server Responsibilities

- Authority over specific portion of the tree
- Maintains the records for the hosts in its tree
- Knows the root servers
  - “Default route”

Name Resolution

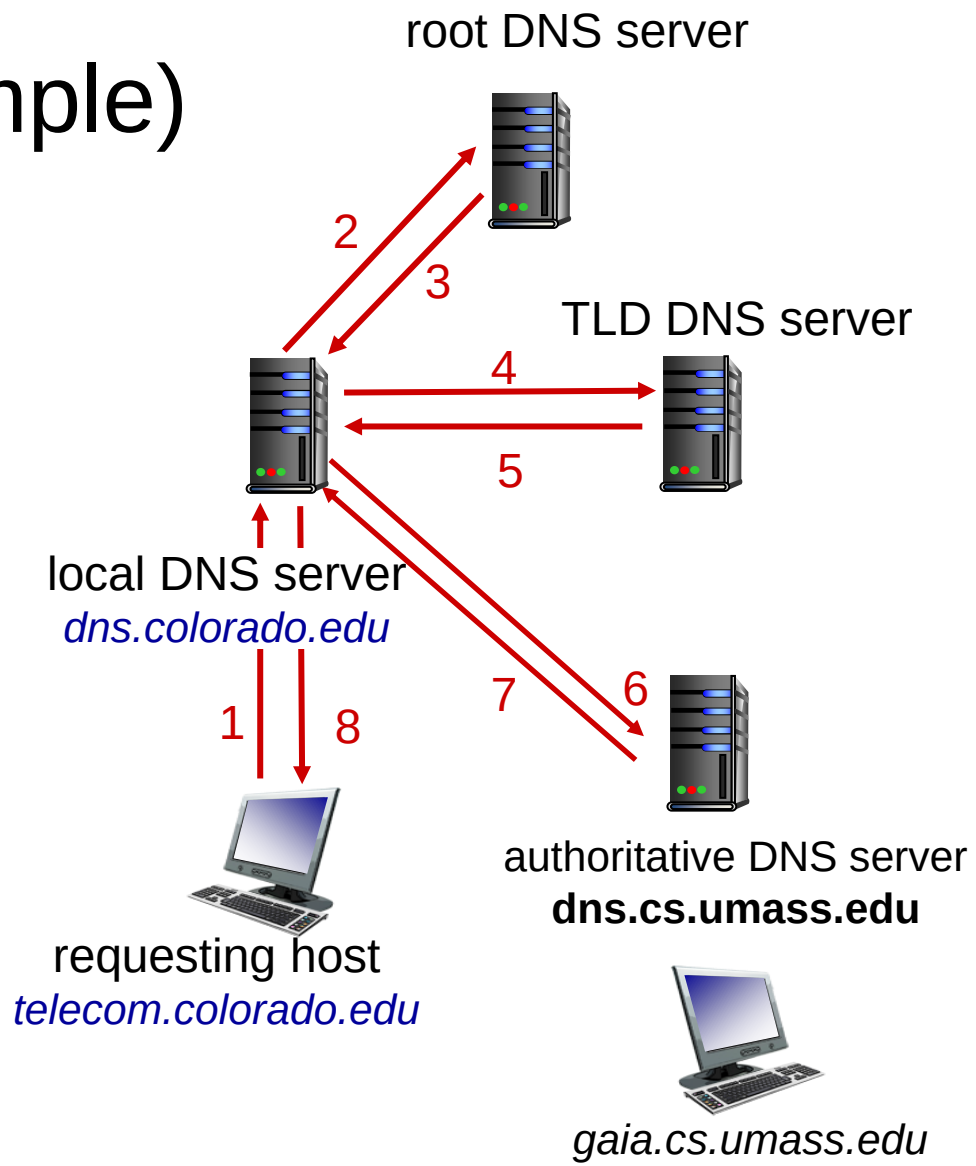
- Every host knows a local DNS server
  - Sends all queries to the local DNS server

- If the local DNS can answer the query, then you're done
  1. Local server is also the **authoritative** server for that name
  2. Local server has **cached** the record for that name

- Otherwise, go down the hierarchy and search for the authoritative name server
  - Every local DNS server knows the root servers
  - Use cache to skip steps if possible
    - ***Skip the root and go directly to .edu if the root file is cached***

DNS Name Resolution (example)

- **Host at cs.colorado.edu wants IP address for gaia.cs.umass.edu**
  - *Iterated query:*
    - ***contacted server replies with name of server to contact***
    - ***"I don't know this name, but ask this server"***



From Host to Server (in detail)

Indirect Advantage of DNS

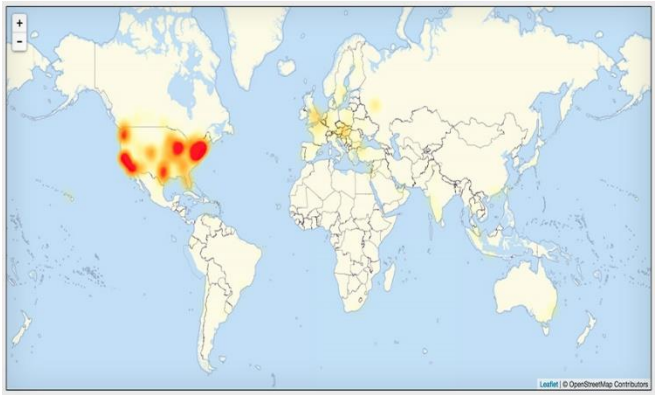
- **Human-readable**

- **Scalability**
  - Many:1
  - 1:many

- **Dynamic DNS**

Dynamic DNS

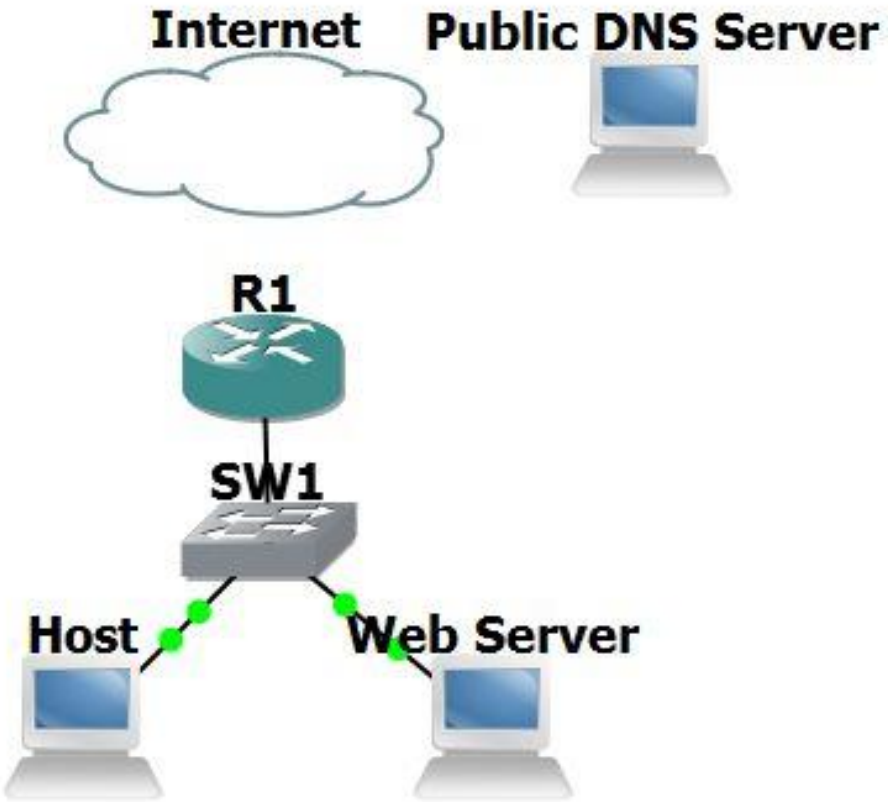
- **Mobile employees**
- **Remote offices**
- **Virtual Private Network (VPN)**
- **dyndns.org**
  - Mirai Botnet 2016



DNS “Hairpin” / Split DNS

- What if the DNS server resolution (Web server) is on the same LAN, the PC uses the public address, and the gateway (router) DNATs?
  - PC Resolves Domain to IP address
  - PC -> HTTP/TCP SYN -> Default-gateway
  - Router -> NAT
  - Server -> HTTP/TCP SYN_ACK -> PC
  - What does the PC do?

DNS “Hairpin” Diagram



DNS “Hairpin” / Split DNS

- **Solutions?**
  - Internal devices point to internal DNS server
  - Router acts as DNS proxy
  - Server on different subnet; DNAT
    - ***Make sure it is placed above the “matchall” NAT***

DNS Records

DNS: **distributed database storing resource records (RR)**

RR format: `(name, value, type, ttl)`

type=A

- **name** is hostname
- **value** is IP address

type=NS

- **`name`** is domain (e.g., foo.com)
- **`value`** is hostname of authoritative name server for this domain/zone

type=CNAME

- **name** is alias name for some "canonical" (the real) name
- **www.ibm.com** is really **servereast.backup2.ibm.com**
- **value** is canonical name

type=MX

- **value** is name of mailserver associated with **name**

Records

- **Address record (A record) – maps hostname to 32-bit IPv4 address**
  - Generally 1x1 mapping of top level domain/subdomain
- **AAAA record (quad A) – maps hostname to 128-bit IPv6 address**
  - Generally 1x1 mapping of top level domain/subdomain
- **Mail exchange record (MX record) – maps a domain to a list of mail exchange servers for that domain**
  - Allows 1xMany mappings
  - Email destined for a particular domain can be routed to one of many listed MX records

Open DNS (Umbrella) and Alternative DNS

- **Bypasses sensors and filters**
- **Speed**
- **Negatives?**

OpenDNS

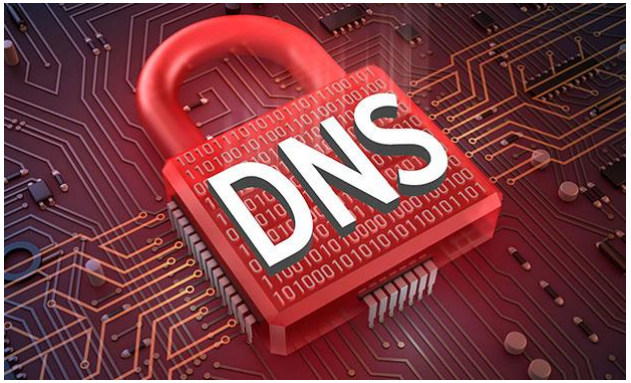
DNS - Security

- **DNS was not designed with security in mind**

- **Trust DNS**
  - mybankaccount.com

- **Spoofing**
  - paypal.com vs. paypa1.com

- **Denial of Service (DoS)**
  - Local – no DNS
  - Server – no domain



- **DNS Hijacking**
  - Virus on OS changes local DNS server: mybankaccount.com to badguybank.com

Security

- **Domain Name Security Extensions (DNSSEC)**
  - Keys for cryptographically signed responses
    - ***Hierarchy of trust within zones***
  - Deployment 2010

- **Device Hardening**
  - DNS Proxy

Interdisciplinary - Politics

- **VeriSign**
  - “Site Finder” Redirecting

- **Unites States political influence over ICANN**
  - .xxx TLD
  - COVID-19

DNS: caching, updating records

- Once (any) name server learns mapping, it *caches* mapping
  - Cache entries timeout (disappear) after some time (TTL)
  - TLD servers typically cached in local name servers
    - ***Root name servers not often visited***
- Cached entries may be *out-of-date* (best effort name-to-address translation!)
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire
- Update/notify mechanisms proposed IETF standard
  - RFC 2136

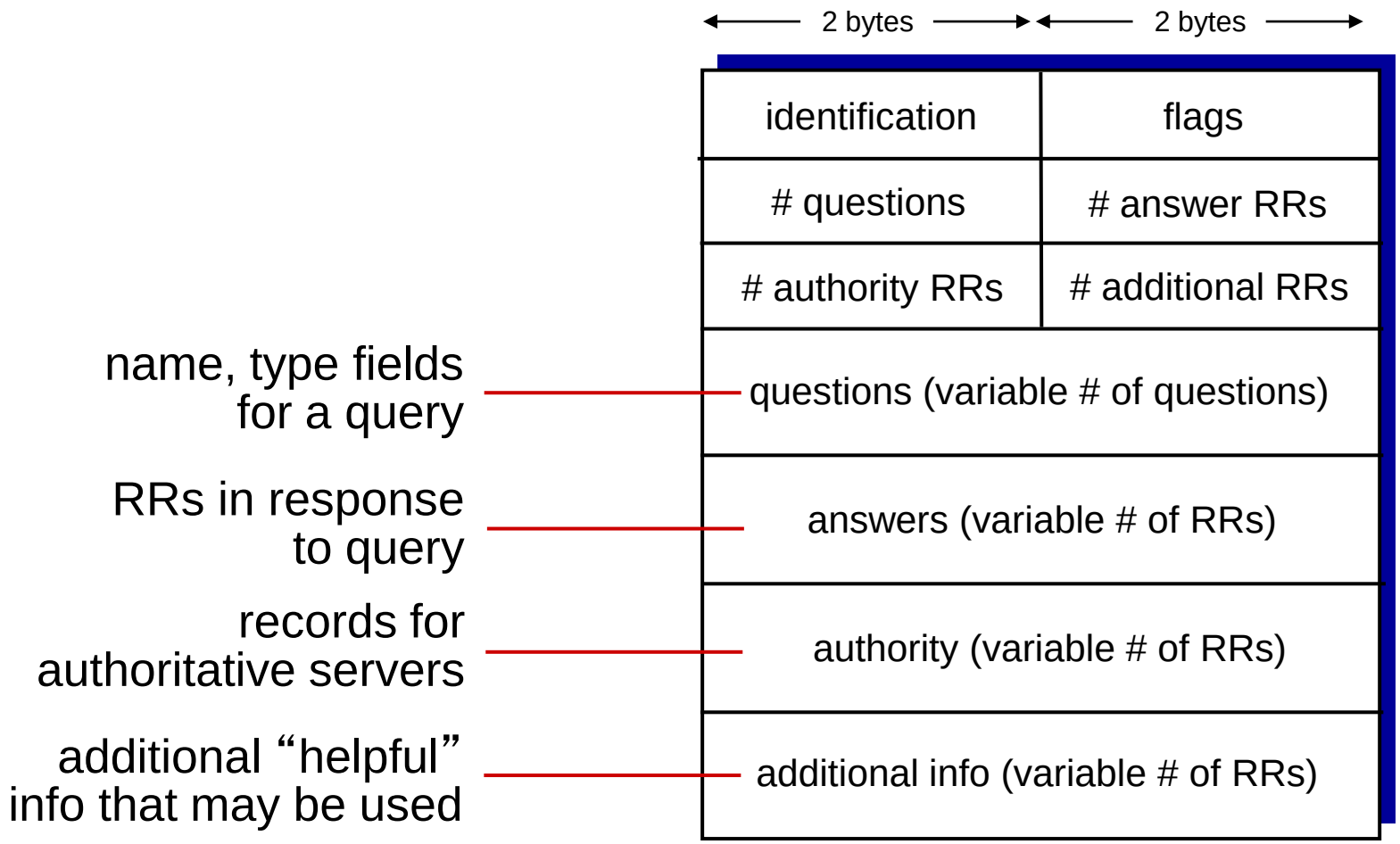
DNS Protocol Messages

- *query* and *reply* messages, both with same *message format*

- Message Header
  - identification: 16 bit # for query, reply to query uses same #
  - flags:
    - query or reply
    - recursion desired
    - recursion available
    - reply is authoritative

← 2 bytes →	← 2 bytes →
identification	flags
# questions	# answer RRs
# authority RRs	# additional RRs
questions (variable # of questions)	
answers (variable # of RRs)	
authority (variable # of RRs)	
additional info (variable # of RRs)	

DNS Protocol Messages



Inserting Records into DNS

- Example: new startup "Network Utopia"
- Register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts two RRs into .com TLD server:
    (networkutopia.com, dns1.networkutopia.com, NS)
    (dns1.networkutopia.com, 212.212.212.1, A)
- Create authoritative server type A record for www.networkuptopia.com; type MX record for networkutopia.com

type=A
- **name** is hostname
- **value** is IP address

type=NS
- **name** is domain (e.g., foo.com)
- **value** is hostname of authoritative name server for this domain/zone

type=CNAME
- **name** is alias name for some "canonical" (the real) name
- **www.ibm.com** is really **servereast.backup2.ibm.com**
- **value** is canonical name

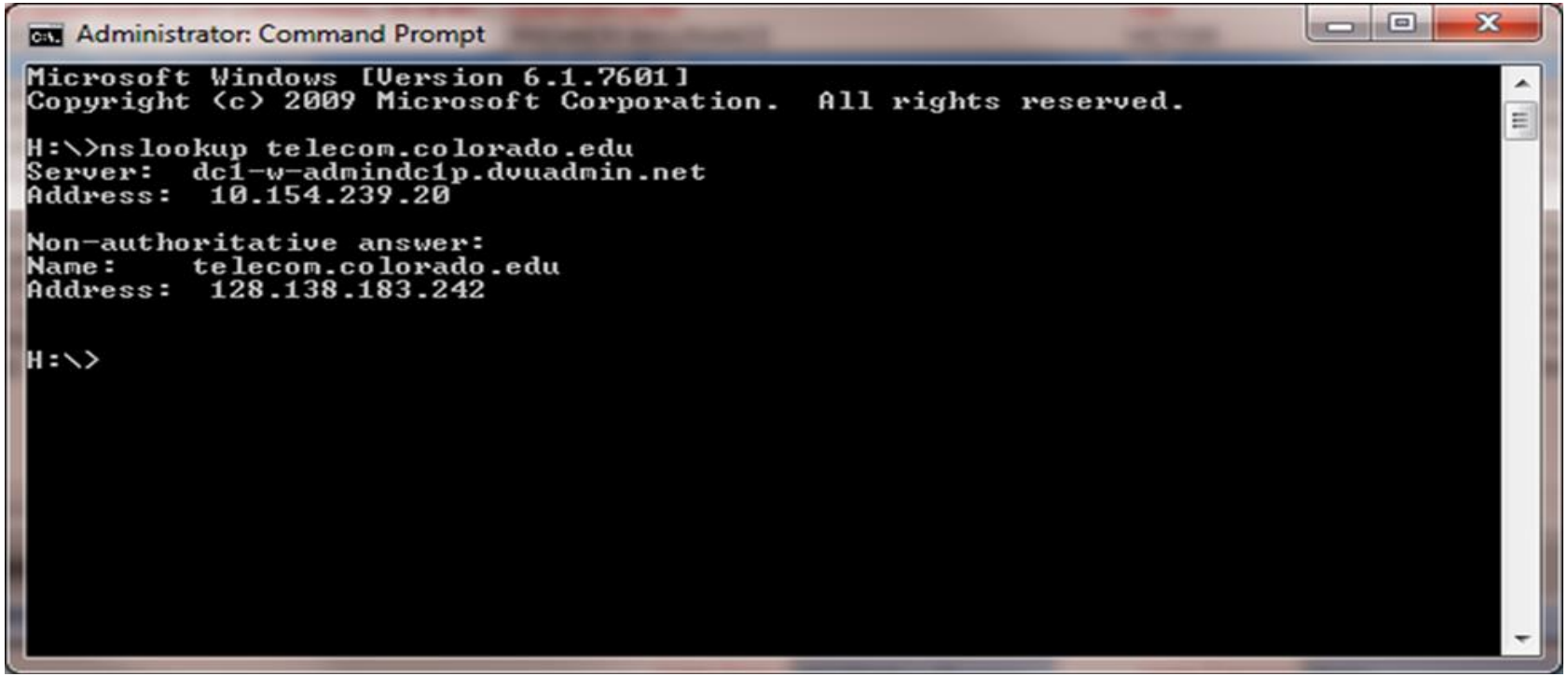
type=MX
- **value** is name of mailserver associated with **name**

Challenge

- **What is the IP address of:**
  - www.raveninnovation.com

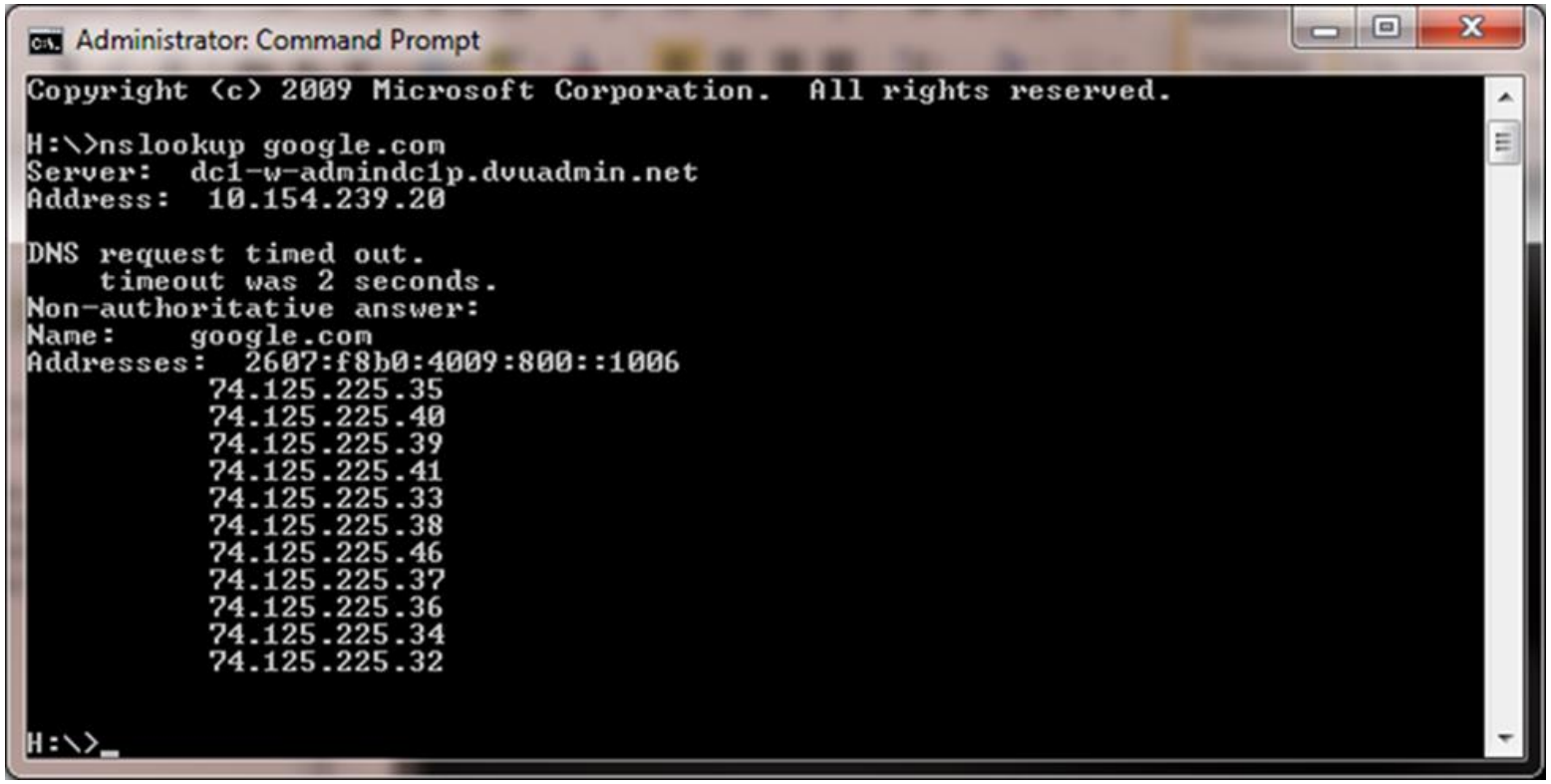
nslookup

- **Troubleshooting Tool**
  - IP address to name resolution



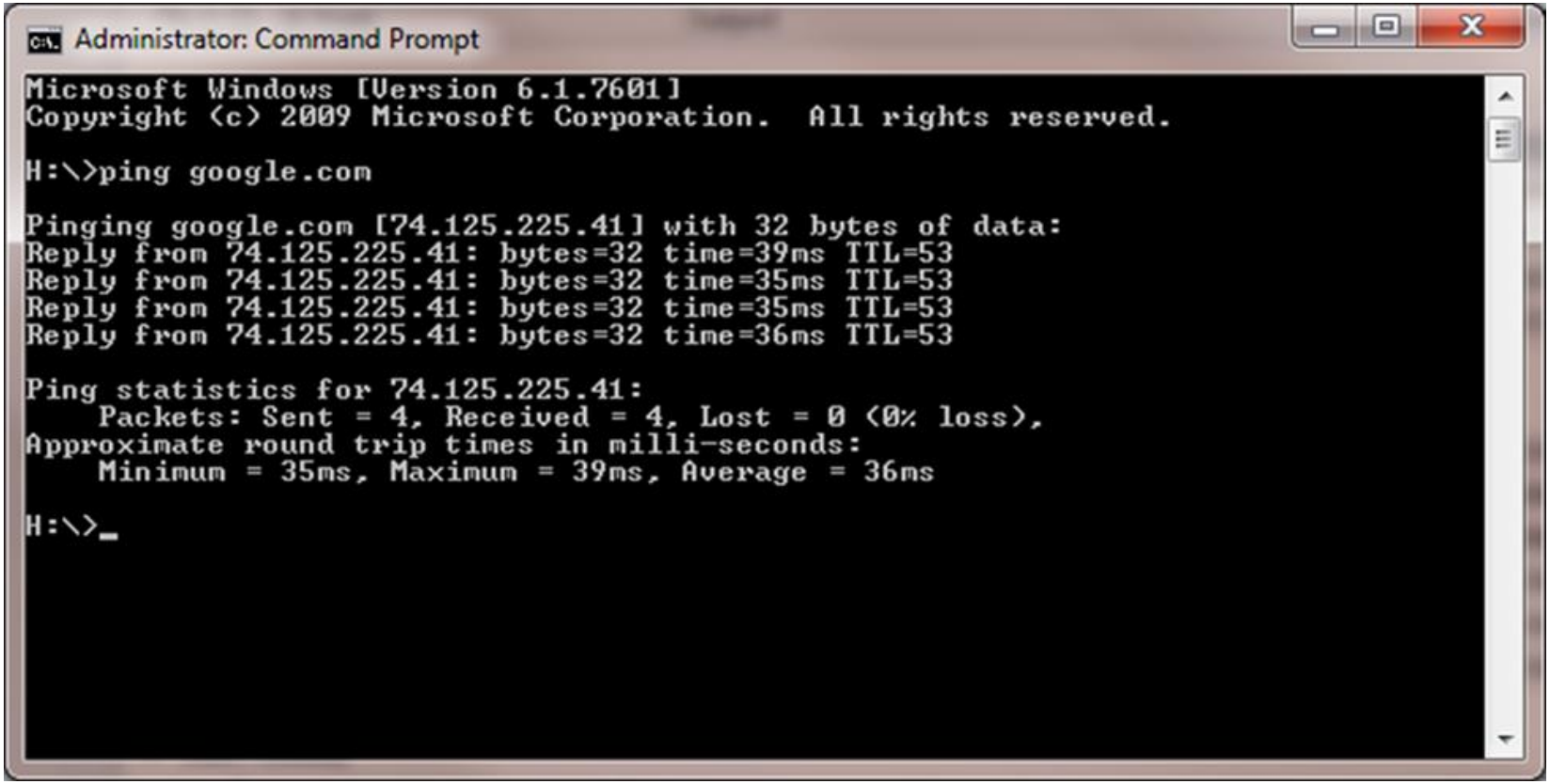
nslookup

- **Multiple IPv4 server addresses**
- **IPv6 address**



Resolution Test

- **Ping domain**



Questions?