Carnegie Mellon University
Software Engineering Institute

IP Addresses and Domain Names

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Department of State under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM19-0683

Learning Objectives

IP Address

Domain Name System (DNS)

IP Address and DNS

Ports

Summary

IP Address -1

Every device (computer, laptop, cell phone, tablet, etc.) connected to a network has an address.

- Comparable to a telephone number
  - One per device
  - Unique world-wide
- Most common form
  - A.B.C.D – called an IP Address (IPv4)
    - Pronounced A dot B dot C dot D or A B C D
    - A, B, C, and D: a number between 0 and 255
    - Read left to right
    - Examples
      - 128.237.30.13
      - 192.88.209.7
      - 23.196.50.167

IP Address -2

“Magic” addresses (aka private addresses)

Think: business PBX (Private Branch Exchange) for telephone

- Many internal (private) telephone numbers
- Few external (public) numbers
- All calls from inside to outside appear to come from one of the public telephone numbers.

Home and company networks work the same way.

- One public address
- Many private addresses
  - Magic – very specific addresses:
    - 10.B.C.D
    - 172.16.C.D
    - 192.168.C.D
- How most home networks work by default

IP Address -3

The current IPv4 address scheme is running out of space.

- The Internet of Things
  - What if everything – EVERYTHING – was on the Internet?
    - Plugs
    - Cabinet locks
    - The refrigerator
    - …

New format coming

- Called IPv6 (Internet Protocol Version 6)
- Examples
  - FE80:0000:0000:0000:0202:B3FF:FE1E:8329
  - FE80::0202:B3FF:FE1E:8329
- You may see this in the field, but it is less likely.

IP Address -4

What then is my current public IP address?

- Examples
  - http://www.showmyipaddress.com/
  - http://showip.net/
  - http://www.google.com/search?q="what is my ip address”
  - Many, many more
  - Check with your management chain to see what if any recommendations they may have

Domain Name System (DNS) -1

Numbers hard to remember

Names easier to remember

First create naming scheme

- Same dot notation, except names not numbe
- Read left to right
- But hierarchy is right to left, like people’s names and address
  - Joe Smith
  - 4500 Fifth Avenue, Pittsburgh, PA, US
- “Is a member of”
- Example
  - www.microsoft.com
  - www.cert.org
  - www.army.mil

Domain Name System (DNS) -2

Everything but the first part is called a domain.

Right most part is called a Top Level Domain.

- Examples
  - .com – Commercial – Worldwide
  - .mil – Military – US
  - .edu – Education - Worldwide
  - .gov – Government - US
  - .mobi – Mobile sites - Worldwide
  - .xxx – Pornographic sites - Worldwide

Top Level Domains can also be countries.

- Examples
  - .us – United States
  - .ru – Russia
  - .tv – Tuvalu (Pacific Island) but they sold it; now TV (www.tbs.tv)
  - .de – Germany (Deutschland)
  - .es – Spain (España)

IP Address and DNS -1

Translate names to numbers and numbers to names

Telephone

- Phone Book
- Printed because it is (somewhat) static
- Translate name to address

Internet

- Domain Name System, or DNS for short
- Not printed because it is very dynamic
- Translate names to IP addresses

Names to numbers examples

- www.cert.org ➔ 128.237.30.13
- www.microsoft.com ➔ 23.196.50.167
- www.army.mil ➔ 143.69.251.141

Most often one-to-one, but not always

Only translate public numbers

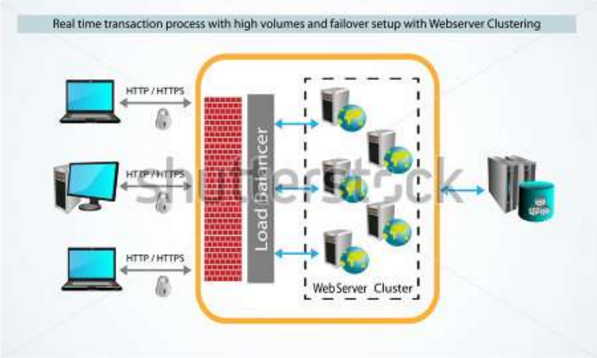
IP Address and DNS -2

“Hold for the next available operator …”

Sometimes many hosts have the same name (www.microsoft.com)

- Load balancing
  - Spread the load over many computers
  - Transparent
- Answer based on question
  - www.google.com - address based on country where lookup originates
    - Translate www.google.com from US gives host in US
    - Translate www.google.com from RU (Russia) gives host In Russia

www.shutterstock.com · 92434231


Real time transaction process with high volumes and failover setup with Webserver Clustering
HTTP / HTTPS
HTTP / HTTPS
HTTP / HTTPS
Load Balancer
WebServer Cluster

www.shutterstock.com · 200889233

www.shutterstock.com · 174393956

DNS Resource Records -1

DNS is a distributed database used to translate hostnames into IP addresses and visa versa, but it has much more information.

Common DNS Resource Records (RR):

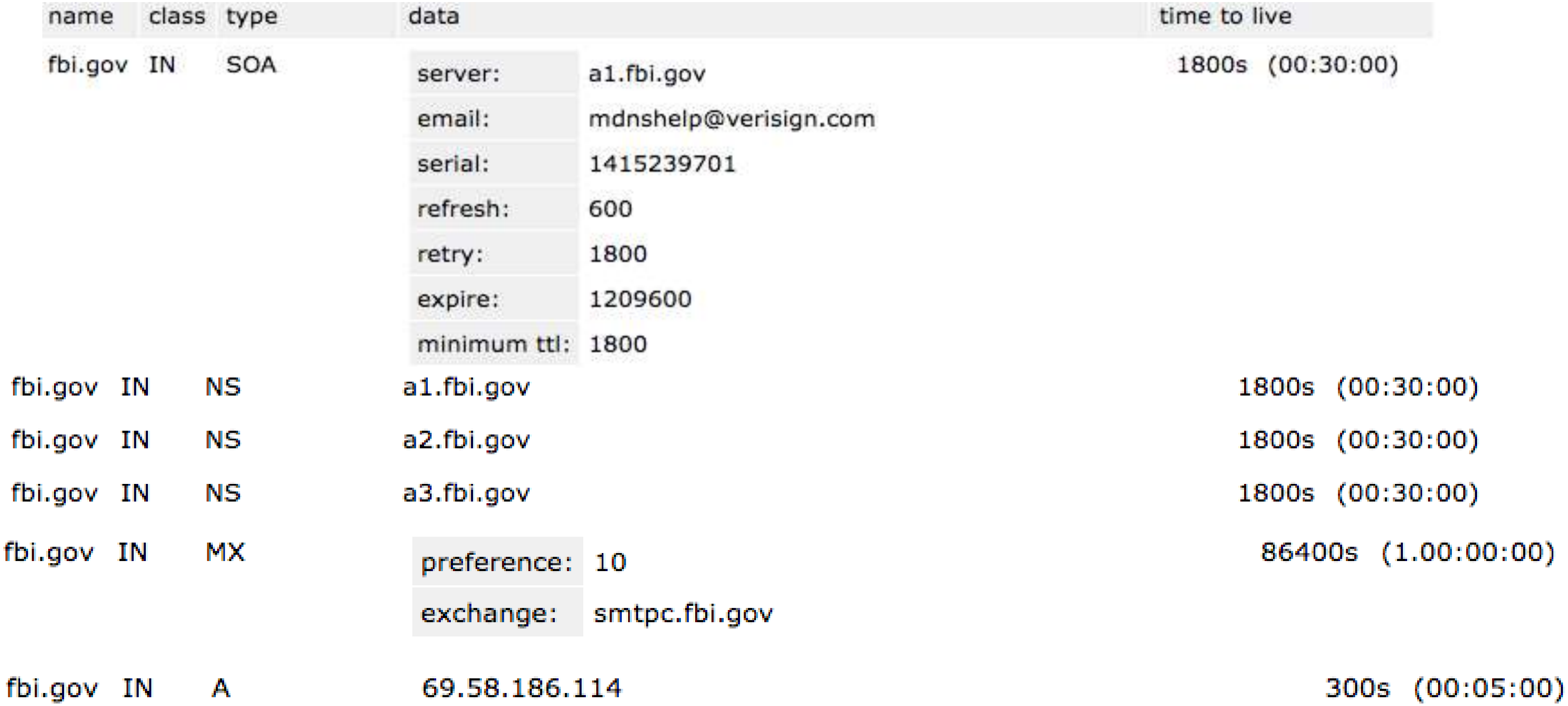
- Address (A) – Map hostname onto IP address(es)
- PoinTeR (PTR) – Map IP address onto hostname, aka an alias
- Canonical NAME (CNAME) – Map hostname alias onto hostname
- Start Of Authority (SOA) – Contact information (mail and email)
- Mail eXchanger (MX) – Host(s) receive mail for domain
- All RRs https://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS Resource Records -2

Useful DNS query websites

- http://www.dnsstuff.com/
- http://centralops.net/co/DomainDossier.aspx
- Many, many more

DNS Resource Records -3



name	class	type	data	time to live
fbi.gov	IN	SOA	server: a1.fbi.gov email: mdnshelp@verisign.com serial: 1415239701 refresh: 600 retry: 1800 expire: 1209600 minimum ttl: 1800	1800s (00:30:00)
fbi.gov	IN	NS	a1.fbi.gov	1800s (00:30:00)
fbi.gov	IN	NS	a2.fbi.gov	1800s (00:30:00)
fbi.gov	IN	NS	a3.fbi.gov	1800s (00:30:00)
fbi.gov	IN	MX	preference: 10 exchange: smtpc.fbi.gov	86400s (1.00:00:00)
fbi.gov	IN	A	69.58.186.114	300s (00:05:00)

Ports -1

Analogy

- Department of Motor Vehicles
  - One street address
  - Many services at that address
    - Driver’s License renewal
    - Title Transfer
    - Registration
    - Etc.
- Network-connected hosts
  - One network address (typically)
  - Many services at that address
    - Web service – port 80 – (http://myhost.mydomain.com)
    - Secure web service – port 443 – (https://myhost.mydomain.com)
    - DNS – 53
    - Whois – 43

Ports -2

Syntax:

- http://host.domain.tld:PortNumber

http://myhost.mydomain.com = http://myhost.mydomain.com:80

https://myhost.mydomain.com = http://myhost.mydomain.com:443

Port numbers are convention, not rules

- Just because the services is running on port 80 doesn’t mean it is web traffic
- Trust but verify

Summary

Hosts need IP addresses to communicate on a network

IPv4 (A.B.C.D) is most prevalent

IPv6 is coming

DNS is a distributed database that maps hostnames to IP addresses and visa versa

DNS contains lots of other data about domains

Hosts provide services at ports