INFO 310

Fall 2016

Week 10 – Lecture 1

HOUSEKEEPING

- Attendance
- Position Paper II:

Assigned today, due 12/6/16

DNS – Domain Name System

- **DNS** is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
- Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide.
- The Domain Name System is an essential component of the functionality of most Internet services because it is the Internet's primary directory service

WIKIPEDIA
The Free Encyclopedia

A brief History

- ARPANET had no equivalent – manual process
  - Hosts.txt
    - /etc/hosts
    - %SystemRoot%\System32\drivers
    - LOCALHOST – 127.0.0.1
    - Vestige: .arpa TLD, in-addr.arpa
- DNS designed in 1983 at UC Irvine
- 1984 birth of BIND (Berkeley Internet Name Domain)
  - Today in Version 9.x, still considered the gold standard, but has viable competitors

Governing Bodies

US Department of Commerce

- *Agency*: National Telecommunications and Information Administration (NTIA)
  - *Delegates to*: Internet Corporation for Assigned Names and Numbers (ICANN)
    - *Operates*: Internet Assigned Numbers Authority (IANA)

Components

- DNS root zone (The “dot”): Contains names and IPs of root servers and authoritative DNS servers for each TLD

- Root Name Servers (13 total, A-M)
  - http://www.root-servers.org
  - BGP Anycast: 632 actual instances as of 10/2016

- TLD – Top-level Domain
  - As of 11/2016: 1519 TLDs
    - (incl. 730 gTLD, 301 ccTLDs)

Components con’t

As of 2015, IANA distinguishes the following groups of TLDs

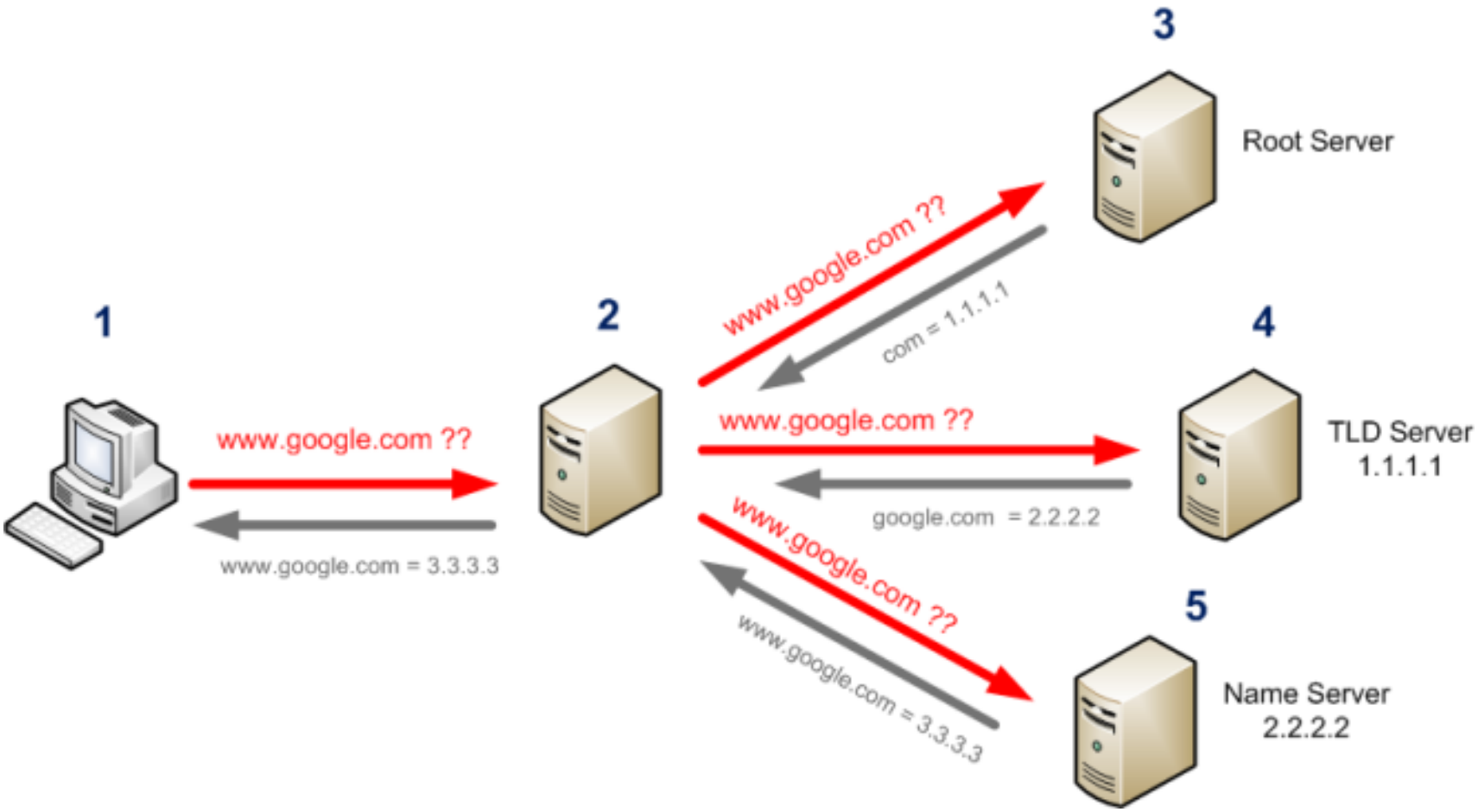
- **infrastructure** top-level domain (ARPA)
- **generic** top-level domains (**gTLD** – com, org, net, …)
- **restricted generic** top-level domains (**grTLD** – biz, name, pro, …)
- **sponsored** top-level domains (**sTLD** - edu, gov, mil, coop, asia, …)
- **country code** top-level domains (**ccTLD** – us, de, se, sov)
- **test** top-level domains (**tTLD** – test, example, invalid, localhost)

Common types of (IPv4) DNS Resource Records

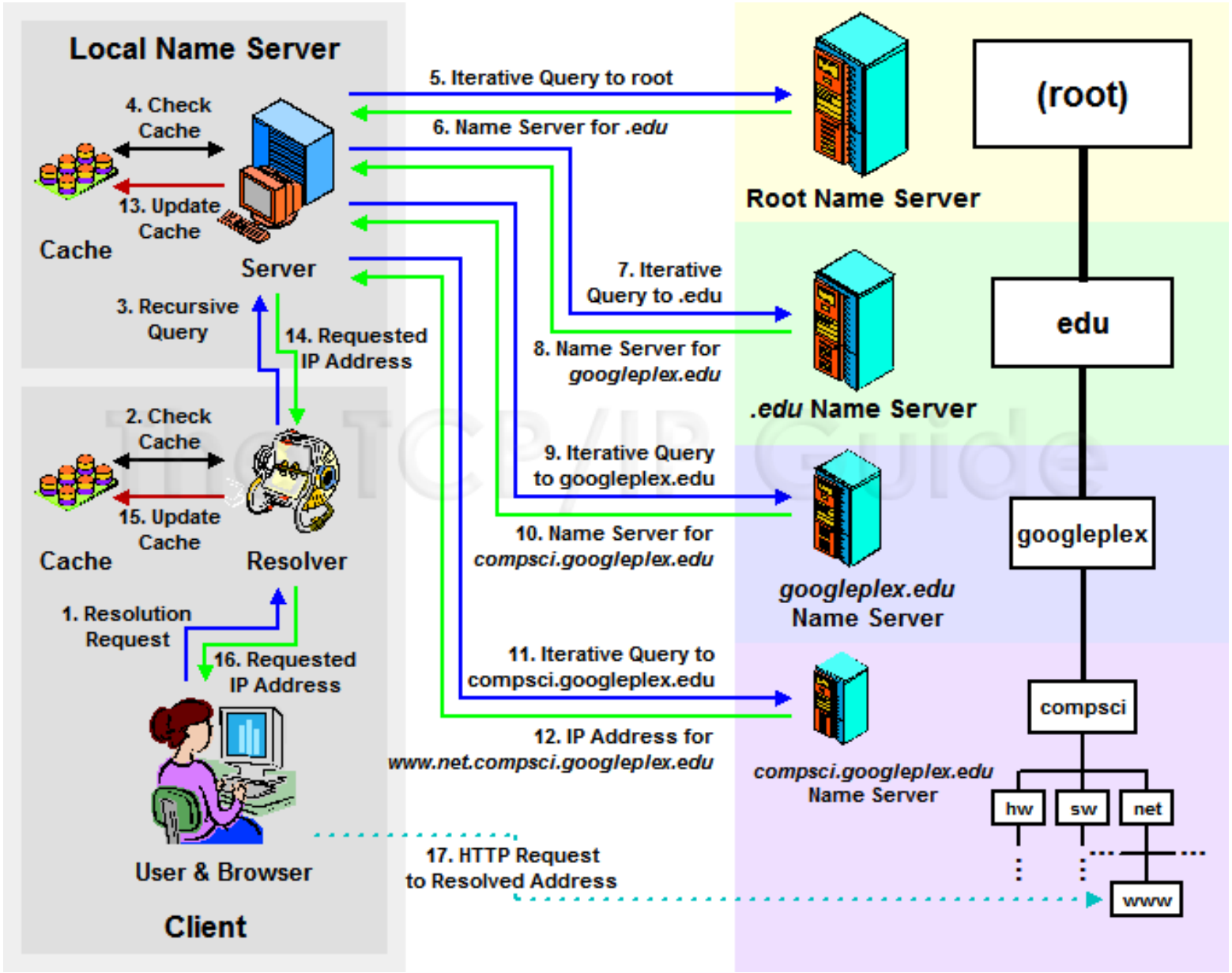
- A – Address Record, points to IP address
- CNAME – Canonical Name Record, always points to another name record, never an IP address. DNS will keep trying with the new name.
- MX – Mail Exchange Record – Which server handles email for the domain
- NS – Name Server Record, authoritative DNS server for the domain
- PTR – Pointer Record, points to a CNAME, but DNS stops there
- TXT – Text Record, arbitrary human readable text
- Not a record, but important: **TTL - TimeToLive**

Types of DNS Servers

- Resolving Name Server (most often caching)
- Root Name Server
- TLD Name Server
- Authoritative Name Servers
  - Primary (master)
  - Secondary (slave)
- Also
  - Caching / Recursive Name Servers (refers to itself first)
  - Alternative roots (alt roots)


1
2
3
4
5
Root Server
TLD Server
1.1.1.1
Name Server
2.2.2.2
www.google.com ??
www.google.com = 3.3.3.3
www.google.com ??
com = 1.1.1.1
www.google.com ??
google.com = 2.2.2.2
www.google.com ??
www.google.com = 3.3.3.3

So you want to browse to www.net.compsci.googleplex.edu



(break)

Firewalls & IDS / IPS: The Traffic Disruption Appliances

- A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.
- Firewalls are often categorized as either *network firewalls* or *host-based firewalls*.

WIKIPEDIA
The Free Encyclopedia

Firewalls cont'd

- 1st gen: Stateless packet filters
- 2nd gen: Stateful traffic inspection
- 3rd gen: Application Layer inspection
  - protocol aware
  - Also called NGFW
- Layer 2 / Transparent vs. Layer 3 / Routed
- Rule based policies
- Hierarchical – allow any any vs. deny any any

IDS / IPS

- Intrusion Detection System
  - Typically passive
  - Mainly for Detection & Alerting
  - Not a critical failure point or choke point
- Intrusion Prevention System
  - Typically active / “in-line”
  - Can affect traffic based on policy
  - Can be critical point of failure
  - Can be throughput choke point

(this page intentionally left blank)

LAB V

- Introduction
- Learning Objective
- Instructions
- Deliverable