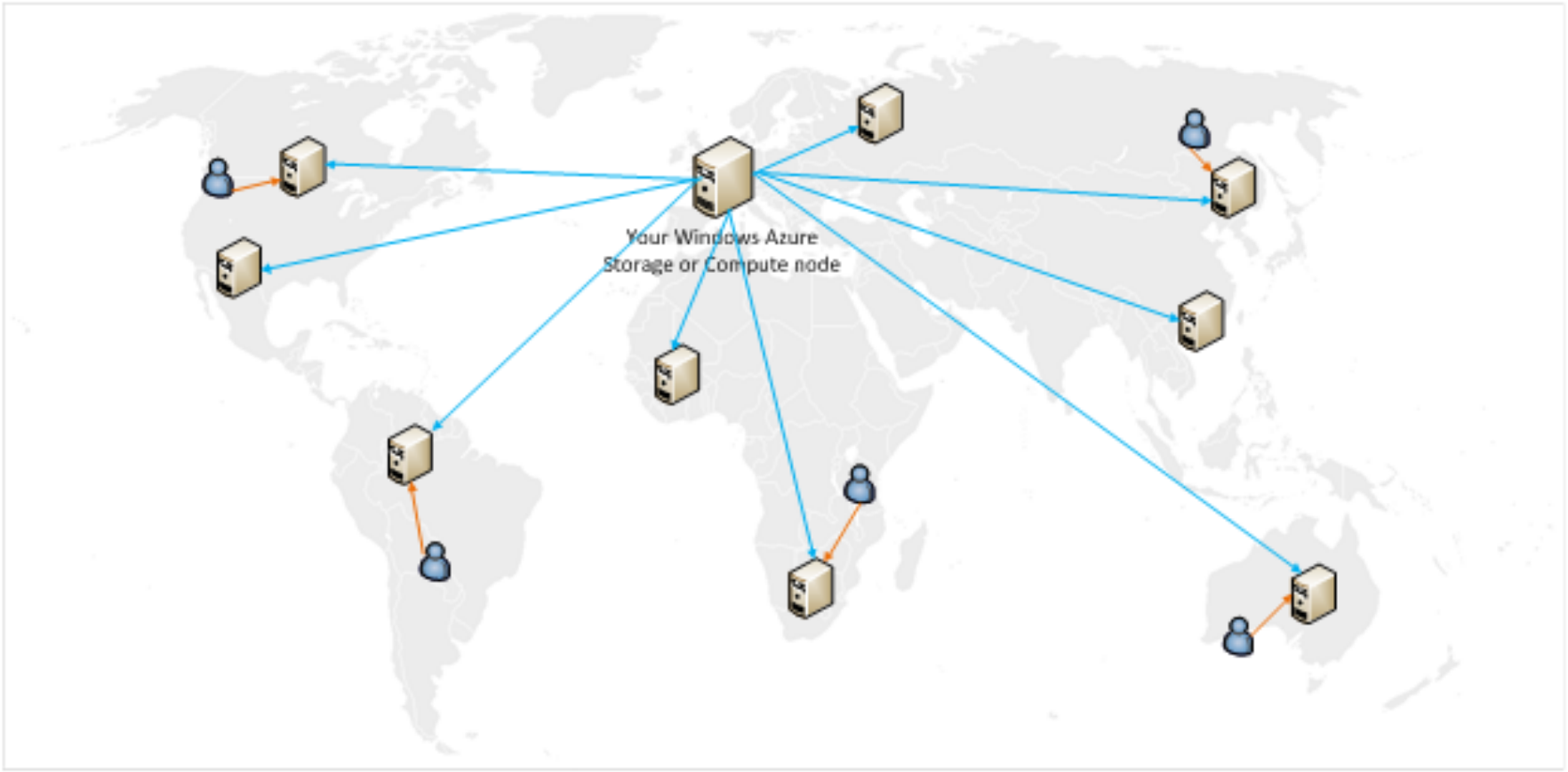
Scaling Static Pages



Slides by Andrew DeOrio

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - Namespace
  - Resolution
  - Administration
  - Scaling and security
- Content delivery networks (CDNs)

Motivation

- You've built a web application that servers one user, the developer
- Runs on the developer's laptop

- How do we scale a web app to many millions of users?
- We need a *production environment*

Development vs. production

- Development environment runs on one computer, sometimes just one program
  - Example: `flask run`
- Production environment is many programs running on many computers
  - Specialized and scalable

- Problem: Where do these computers go?
- Solution: Buy servers

On-premises servers

- Buy your own servers
- Build your own datacenter
- AKA "private cloud"
- AKA "on-premises"

Review: datacenter

- Special building full of computers

- Tons of power
- Tons of internet bandwidth
- Special cooling system
- Lots of computers means lots of computer failures

On-premises to IaaS

- Problem: on-premises physical servers are a pain
  - Keep the AC and power working
  - Backup and failover
  - Replace broken servers
  - Hire engineers and technicians
- Solution: Rent computers

Infrastructure as a Service (IaaS)

- *Infrastructure as a Service (IaaS):* Rent a computer in somebody else's datacenter
  - Might be a virtual machine (more on that next time)
- Benefits
  - Physical datacenter handled by someone else
  - Backups and failover handled by someone else
  - Instantly and automatically rent more computers
- Examples:
  - AWS EC2
  - Google Compute Engine
  - Microsoft Azure Virtual Machines

IaaS to PaaS

- Problem: Managing software on many rented computers is a pain
  - Security updates, complex configuration
- Solution: Rent computers with software already installed and configured

Platform as a Service (Paas)

- *Platform as a Service (PaaS):* Rent a computer in somebody else's data center
  - They manage and configure the software
- Example: servers with database already installed
  - AWS Relational Database Service (RDS)
  - Google Cloud SQL
  - Microsoft Azure SQL
- We'll see many more examples during the next few lectures

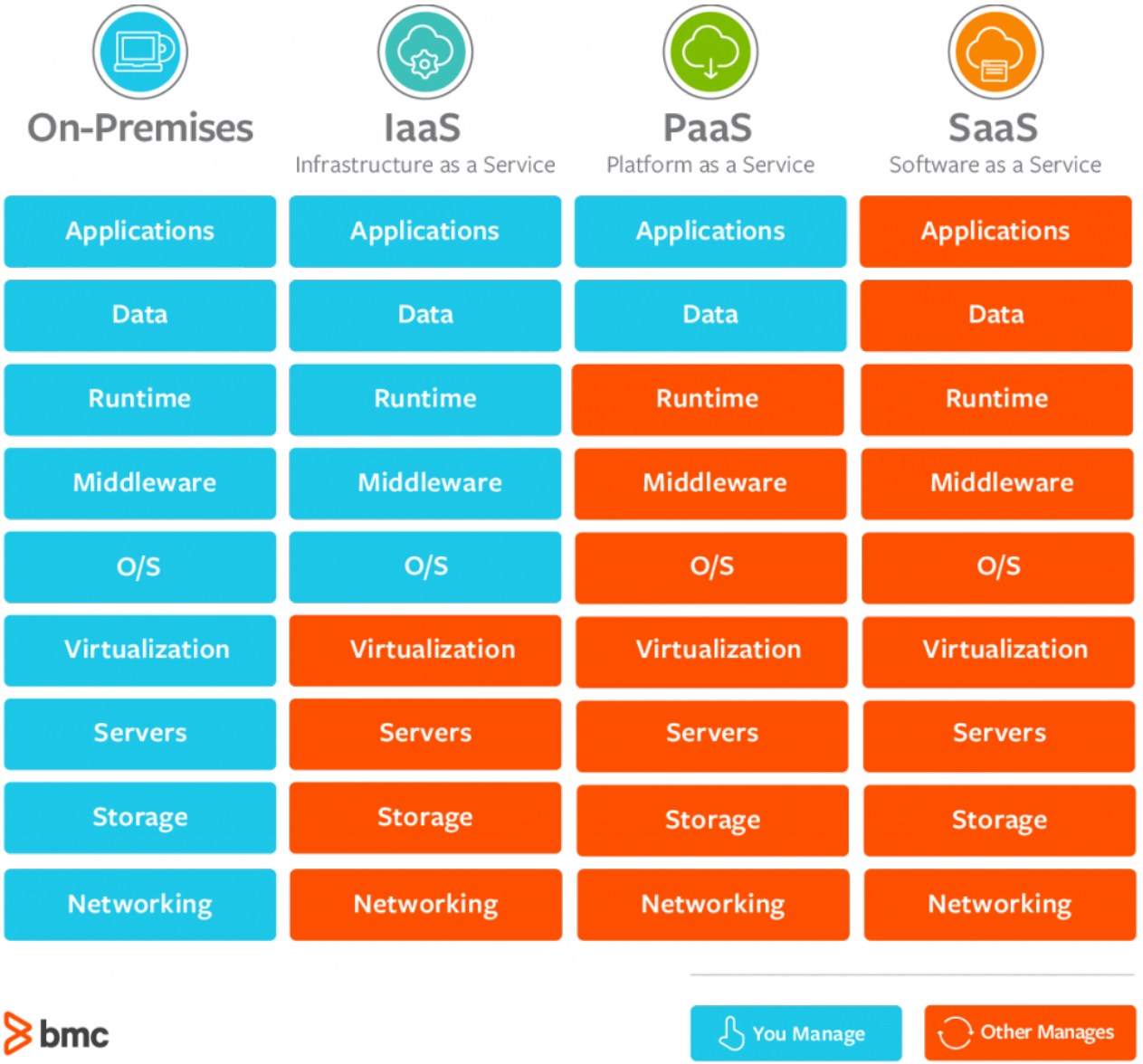
PaaS to SaaS

- Problem: Don't want to write an app, don't want to run an app on rented servers. Just want to use app.
- Solution: Rent a web app running on somebody else's computers

Software as a Service (SaaS)

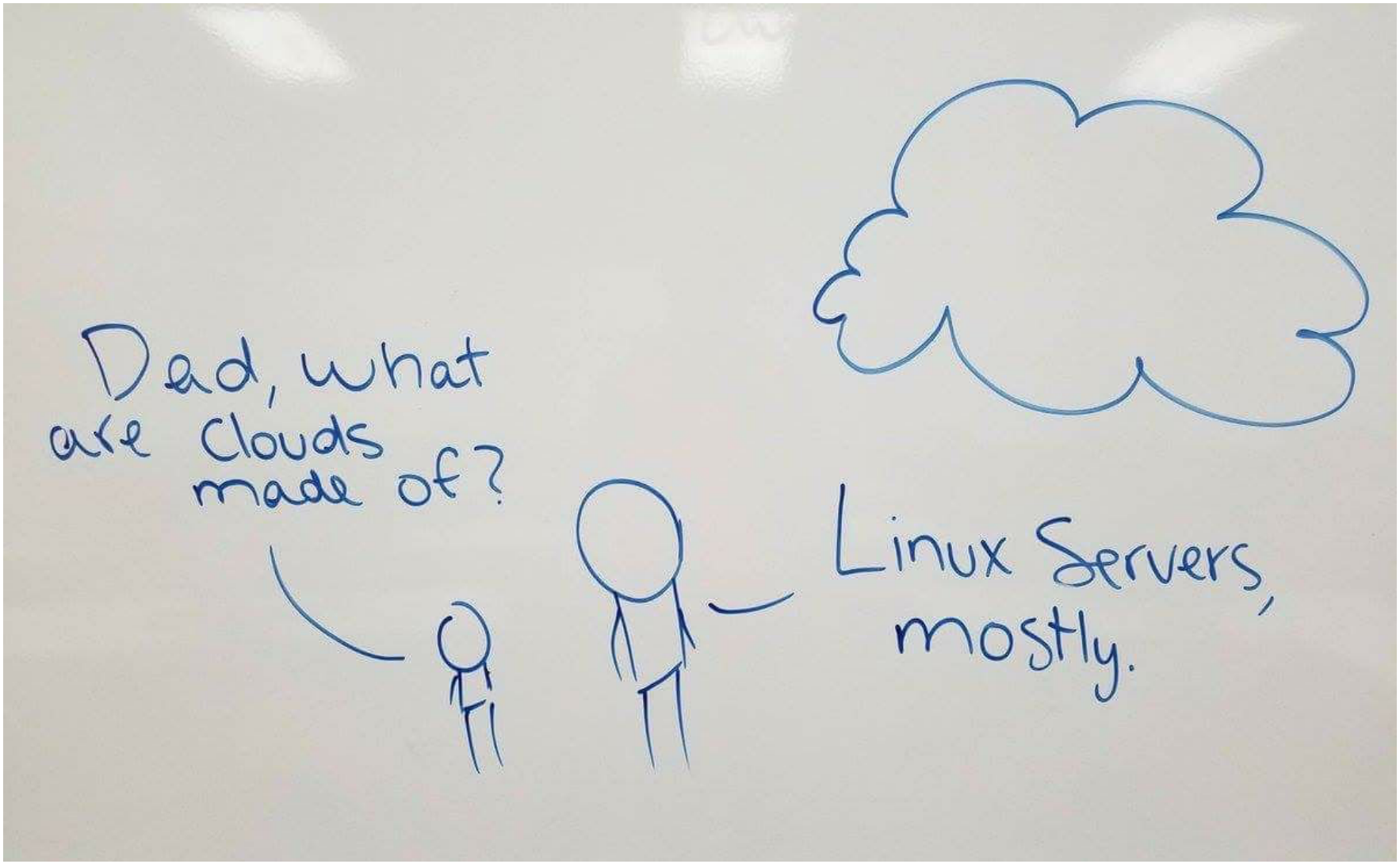
- *Software as a Service (SaaS):* Rent a web app built, hosted, and maintained by somebody else
  - Zero effort
- Examples:
  - Microsoft Office 365
  - Dropbox
  - GitHub
  - Gmail

IaaS vs. PaaS vs. SaaS



https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Cloud memes

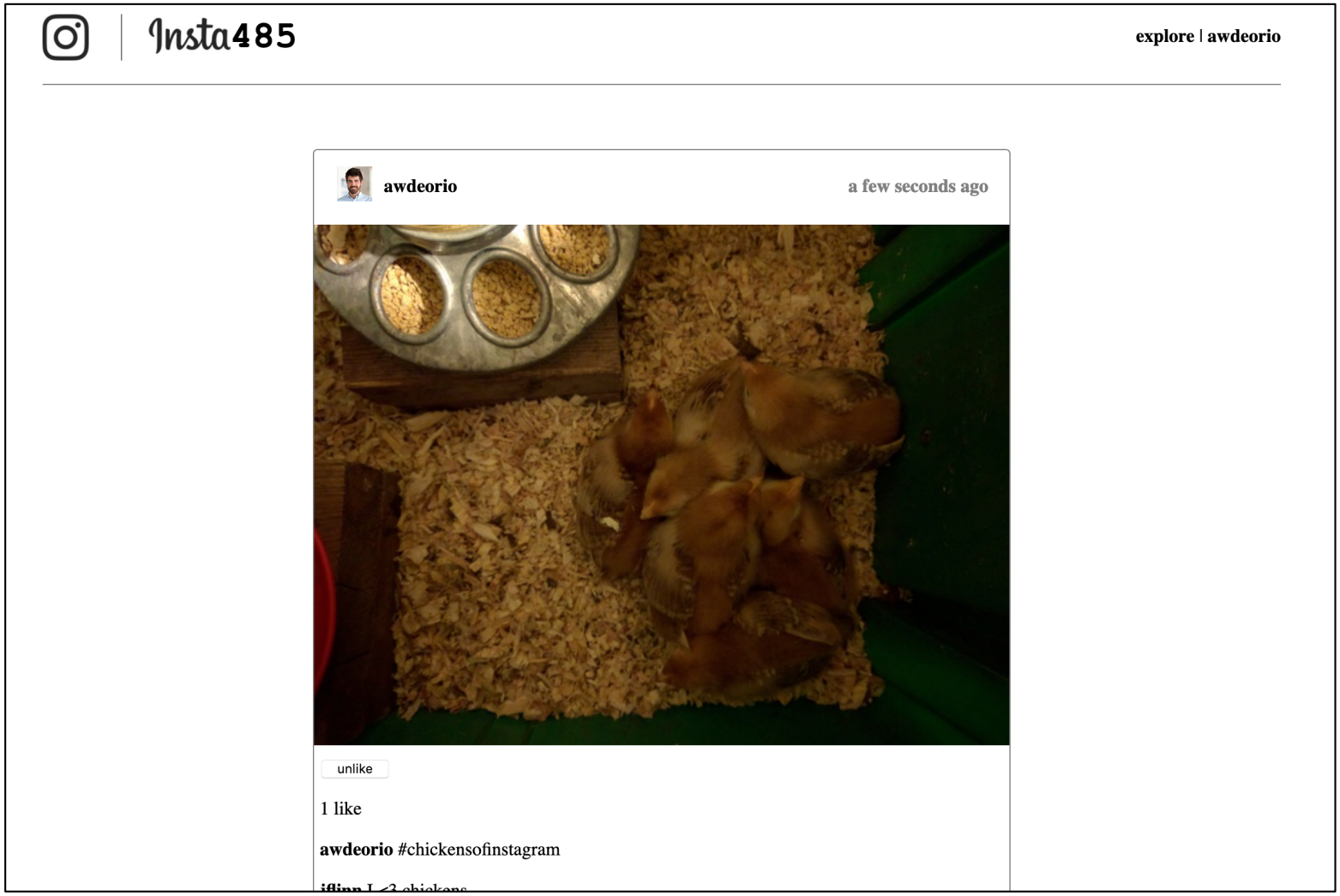


Cloud memes

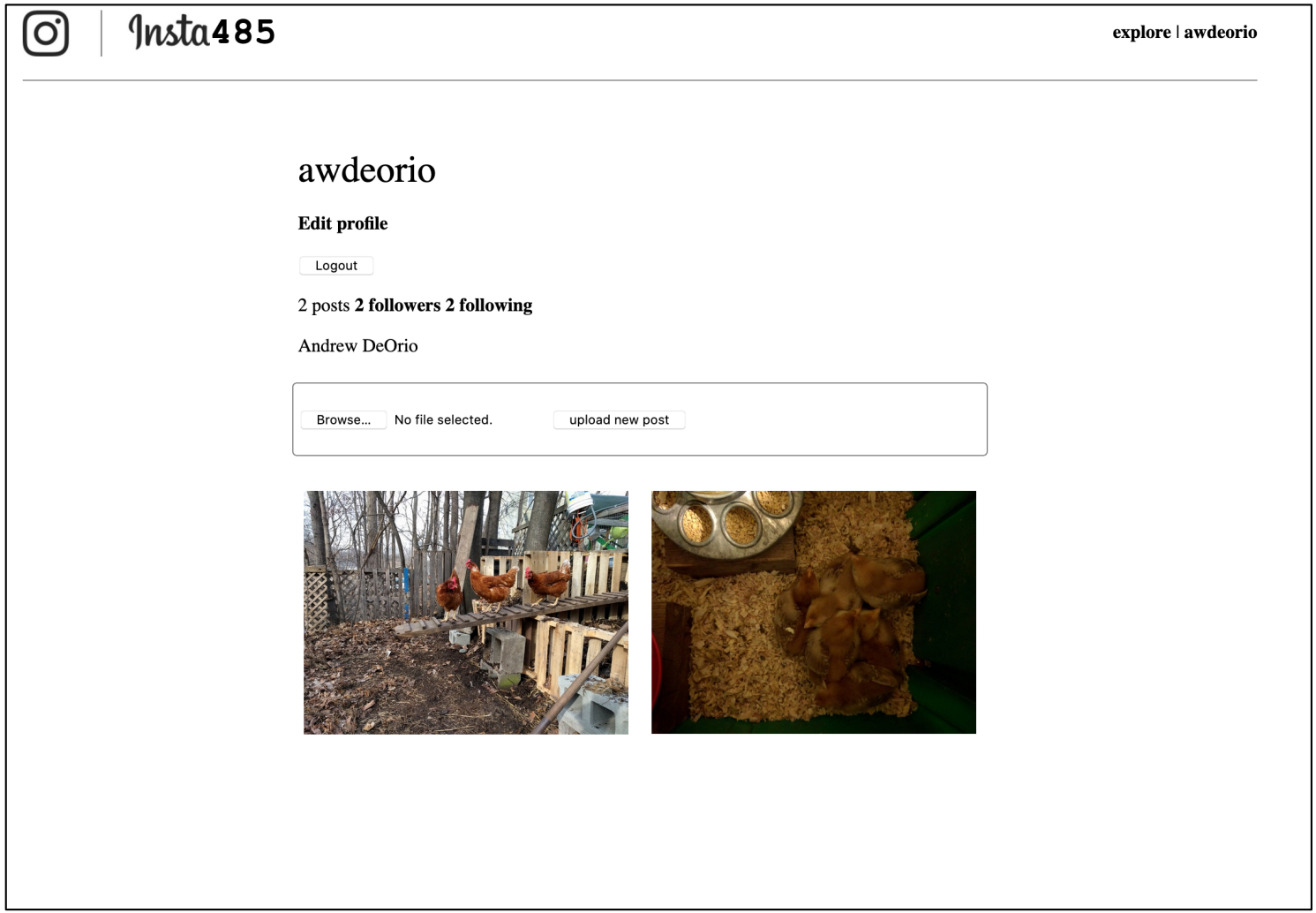
Web apps in the cloud

- Problem: How do I run my web app in the cloud?
- Scale one thing at at time
  - Static pages
  - Server-side dynamic pages
  - Client-side dynamic pages
  - Database storage
  - Media uploads storage
- Use any combination of on-premises servers, IaaS, and PaaS

Static pages, server-side dynamic pages, client-side dynamic pages



Database storage, media uploads storage



Agenda

- Cloud
- **Scaling static pages intro**
- Domain name system (DNS)
  - Namespace
  - Resolution
  - Administration
  - Scaling and security
- Content delivery networks (CDNs)

Static pages

- Static pages: a request returns a copy of a file

- Problem: How do we serve copies to many clients at the same time?
- Solution: many servers

- Problem: It takes a long time for a request/response to traverse the global internet
- Solution: servers in different geographic locations

Review: Internet Protocol (IP)

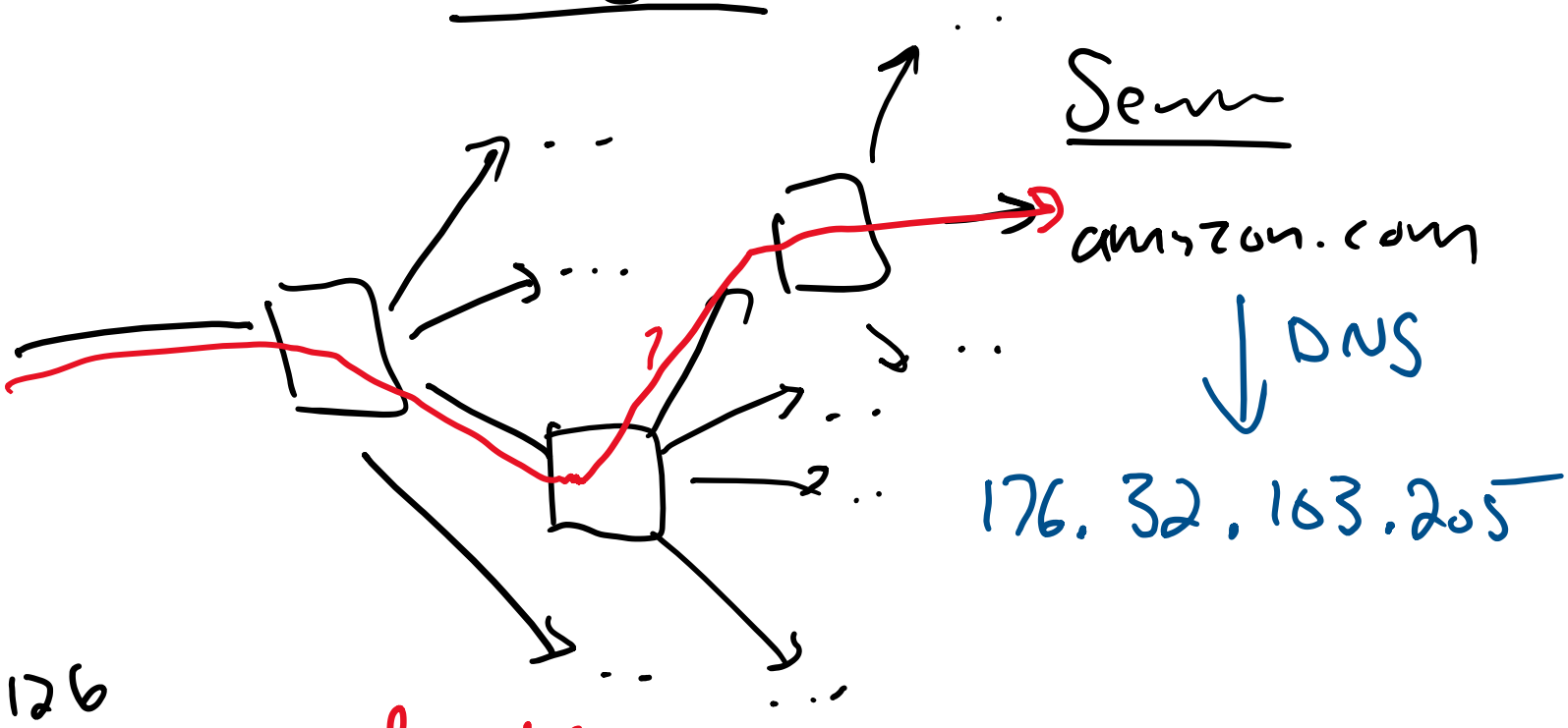
- How does information travel to the right place?

- Every computer on the Internet has an address
  - Google 172.217.5.14
  - Amazon 205.251.242.103
  - My laptop 141.212.109.1

- Newer version: longer addresses
  - IPv4: 32 bits is 4 billion computers
  - IPv6: 64 bits is way more

traceroute google.com → 9 hops

Review: IPv4 routing



More *hops* to far-away servers. Request and response takes longer.

DNS directs to different regions

- Locate many servers in different geographic regions
- Direct clients to the IP address of a nearby server using DNS

- How does DNS work?

Agenda

- Cloud
- Scaling static pages intro
- **Domain name system (DNS)**
  - Namespace
  - Resolution
  - Administration
  - Scaling and security
- Content delivery networks (CDNs)

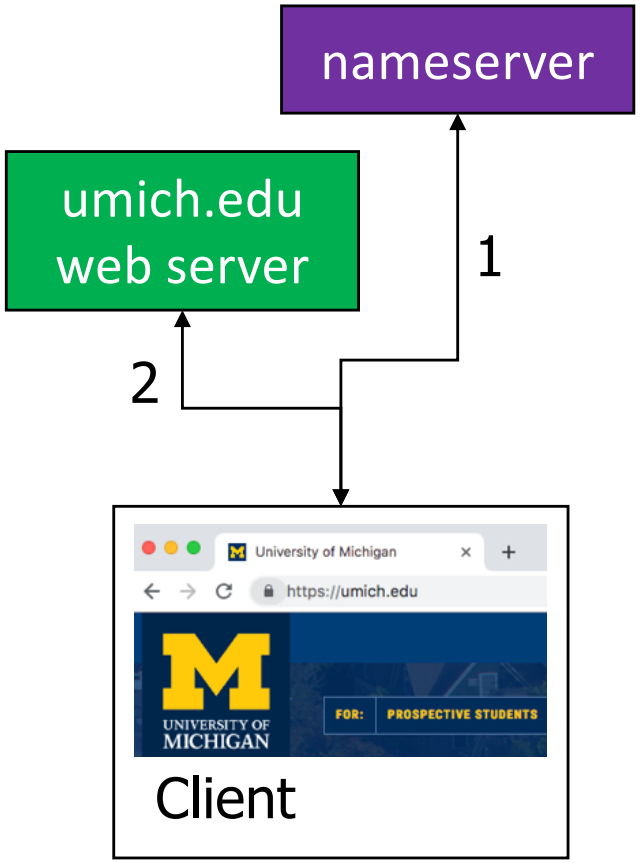
Domain Name System (DNS)

- The Domain Name System (DNS) translates domain names to IP addresses
- Basically a database of (hostname, IP) pairs
- `umich.edu -> 141.211.243.251`

DNS requirements

- Needs to be up all the time
- Continuously updated by many parties
- Must be accurate; errors prevent connections
- Serves massive query load
- Distributed administration

DNS example



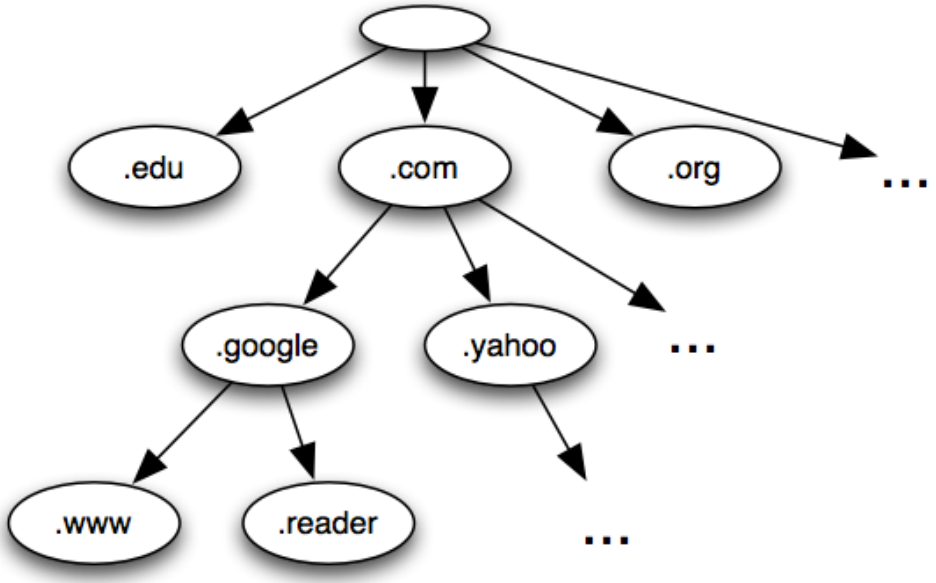
Nameserver
provides IP of
umich.edu

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - **Namespace**
  - Resolution
  - Administration
  - Scaling and security
- Content delivery networks (CDNs)

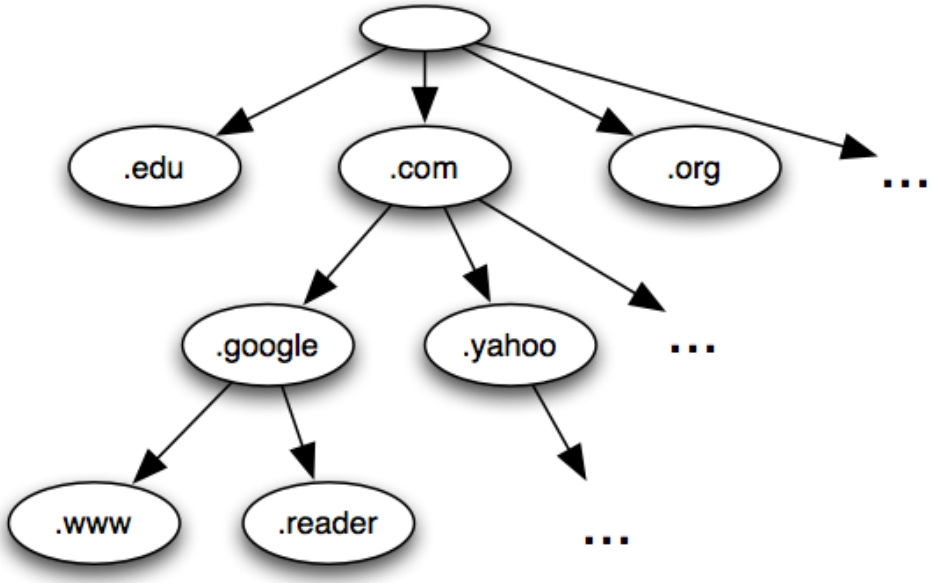
The namespace

- Domain names must be unique, need a namespace
- Tree structure, 1-63 chars per node
- *Fully-qualified domain name* is leaf-to-root name
- Only *DNS root* has no parent



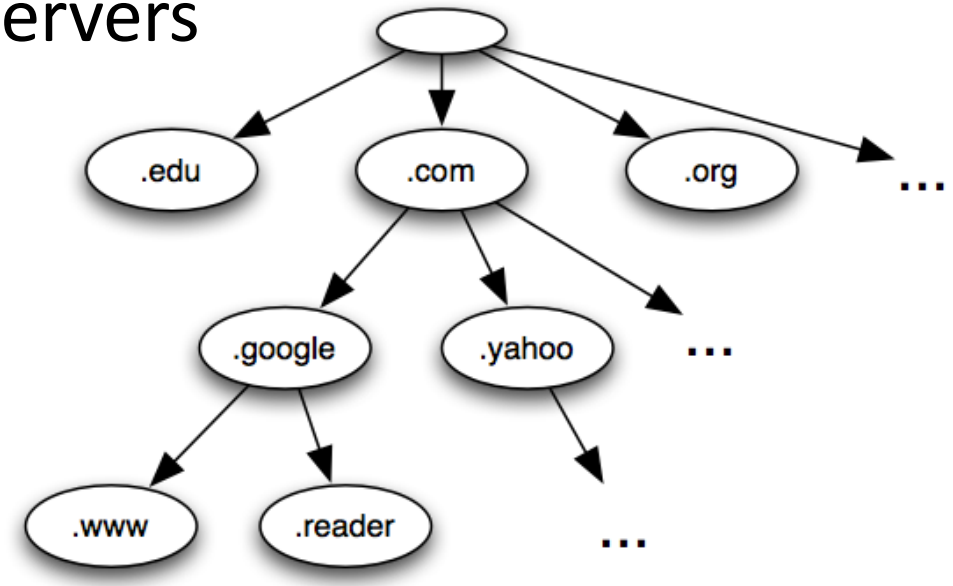
The namespace

- Each node is usually a server running DNS server software



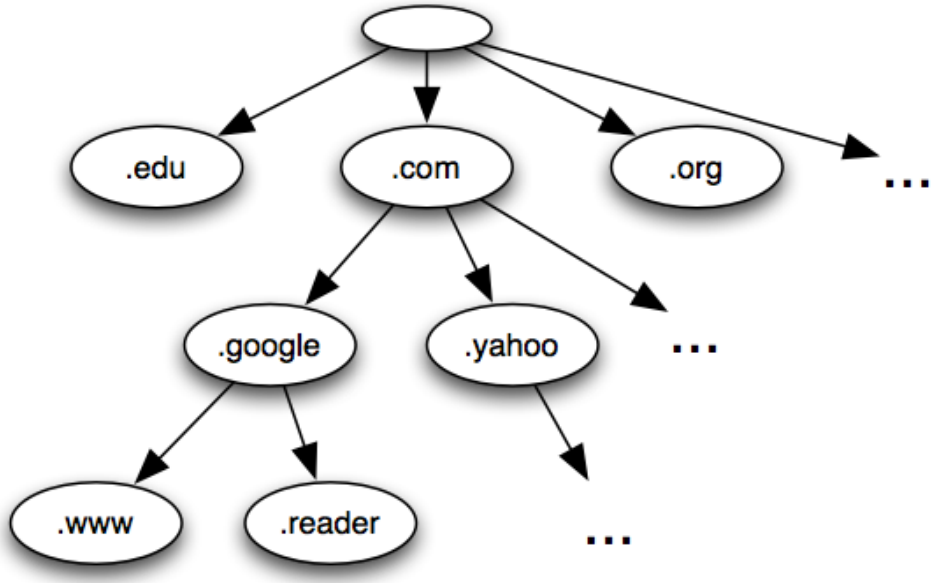
The namespace

- Nodes grouped into administrative zones
  - E.g., root, com, google.com
- Each zone served by authority servers
  - AKA authoritative name servers
- Authority server can delegate subdomains to other authority servers



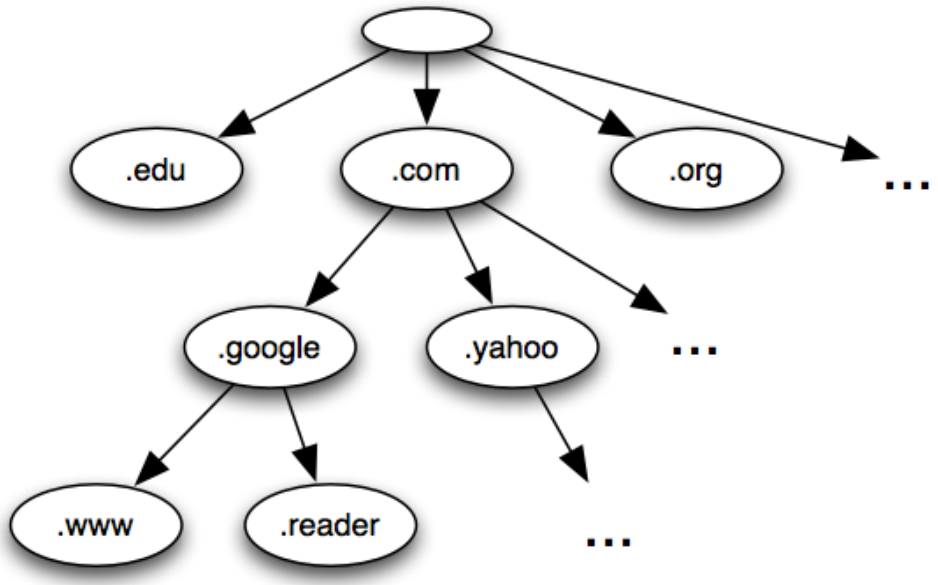
The namespace

- Servers are primary or secondary
  - Primary authority servers are given content by admins
  - Secondary authority servers grab from primaries
- A domain registrar inserts your name into the primary authority server for .com (or .net, .org, etc)



The namespace

- Purchased domain names inserted into 1 primary, 1 secondary (in case of primary failure)



Try it yourself

- Check if a domain name is registered

```
$ whois umich.edu
...
Registrant:
   University of Michigan -- ITD
   ITCS, Arbor Lakes
   4251 Plymouth Road
   Ann Arbor, MI 48105-2785
   UNITED STATES
...
Domain record activated:    07-Oct-1985
Domain record last updated: 14-Feb-2014
Domain expires:             31-Jul-2017
```

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - Namespace
  - **Resolution**
  - Administration
  - Scaling and security
- Content delivery networks (CDNs)

Resolution

- Content of DNS consists of *resource records*
  - Host -> IP
- Most DNS activity
  - Client requests to authority servers
  - Server responds with resource record
- DNS clients built into network libraries
  - Clients use UDP (not TCP) to grab data
  - If your connection is taking a long time to establish, possibly waiting for DNS

Resolution in practice

- Query your DNS server: what is the IP address for `umich.edu` ?

```
$ host umich.edu
umich.edu has address 141.211.243.251
```

Where do I get a DNS server?

- IP addresses are commonly assigned automatically
  - When you connect to a wifi or wired network
- DHCP: Dynamic Host Configuration Protocol
  - Assigns an IP
  - Provides DNS servers

```
$ cat /etc/resolv.conf
# This file is automatically generated.
domain eecs.umich.edu
nameserver 141.213.4.4
nameserver 141.213.15.4
nameserver 10.10.10.10
```

Yes, it's spelled "resolv"

Resolution with more detail

- More detailed DNS resolution

```
$ dig umich.edu
...

;; QUESTION SECTION:
;umich.edu.                    IN    A

;; ANSWER SECTION:
umich.edu.       87    IN    A     141.2
...

;; Query time: 1 msec
;; SERVER: 141.213.4.4#53(141.213.4.4)
;; WHEN: Fri Mar 29 09:58:36 2019
;; MSG SIZE  rcvd: 203
```

IP for `umich.edu`, same as reported by `host`

One of the DNS servers in `/etc/resolv.conf`

Resolution with more detail

- In the previous example, our DNS server had a cached copy of the IP address for `umich.edu`
- What if it didn't have a cached copy?
- Ask the authority servers

```
$ dig umich.edu
...
umich.edu.      87    IN    A     141.211.243.251
...
;; SERVER: 141.213.4.4#53(141.213.4.4)
```

Resolution with more detail

- Ask the authority servers

1. Local nameserver knows IP of root DNS servers
2. Local nameserver queries root DNS servers to get IP address of edu DNS servers
3. Local nameserver queries edu DNS servers to get IP of umich.edu DNS servers
4. Local nameserver queries umich.edu DNS server
5. Response from umich.edu DNS servers includes final answer

Resolution

```
$ dig +trace umich.edu
. 453944 IN NS j.root-servers.net
;; Received 492 bytes from 141.213.4.4

edu. 172800 IN NS d.edu-servers.net
;; Received 486 bytes from 192.58.128.30

umich.edu. 86400 IN NS dns1.itd.umich.edu
;; Received 203 bytes from 192.31.80.30

umich.edu. 1800 IN A 141.211.243.251
;; Received 43 bytes from 192.12.80.214
```

Local nameserver provides IP of **root DNS server**

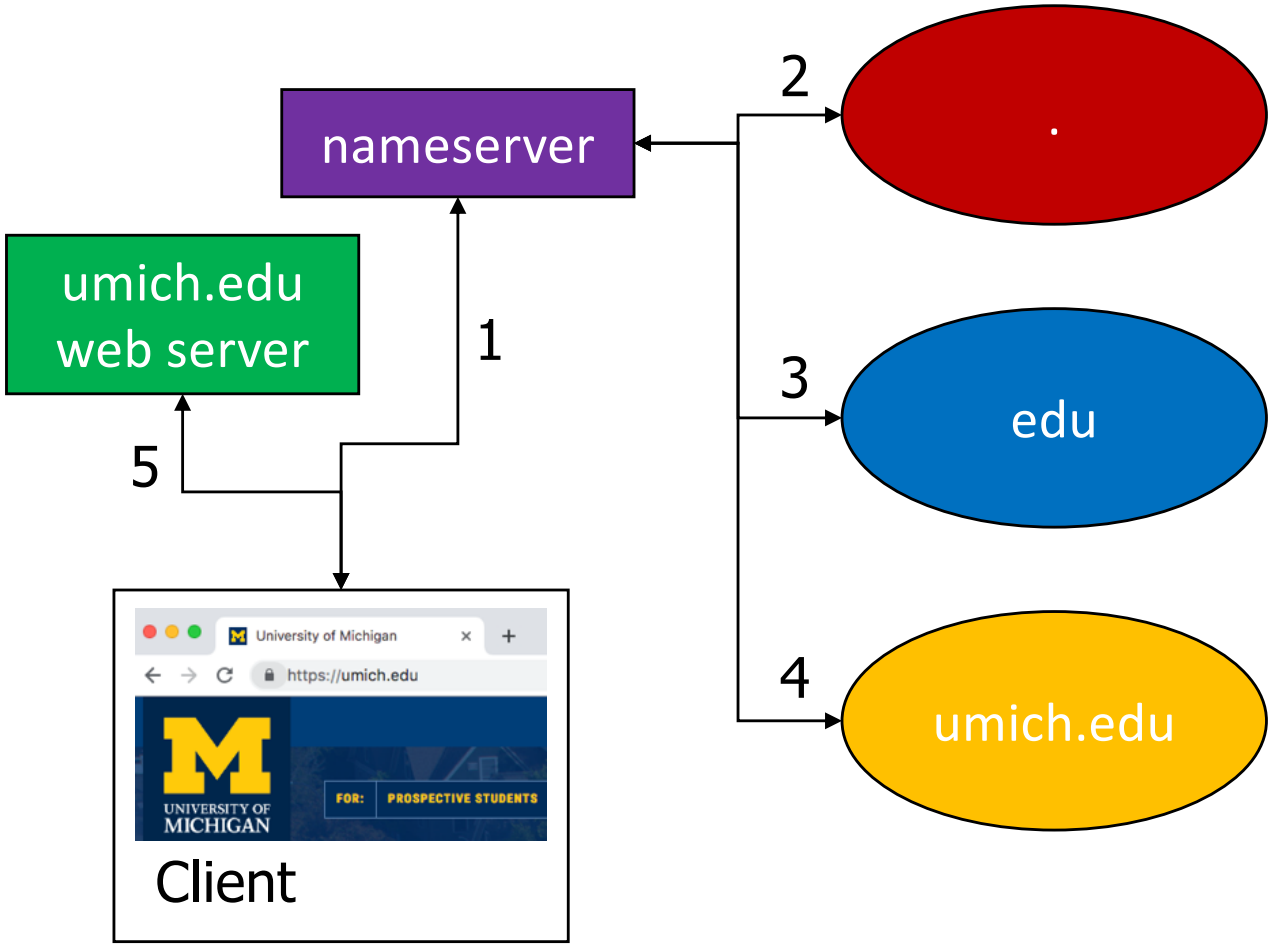
root DNS server provides IP of **edu DNS server**

edu DNS server provides IP of **umich.edu DNS server**

umich.edu DNS server provides IP of **umich.edu**

Note: output is simplified. Try `dig +trace +all umich.edu` for EVERYTHING.

Resolution



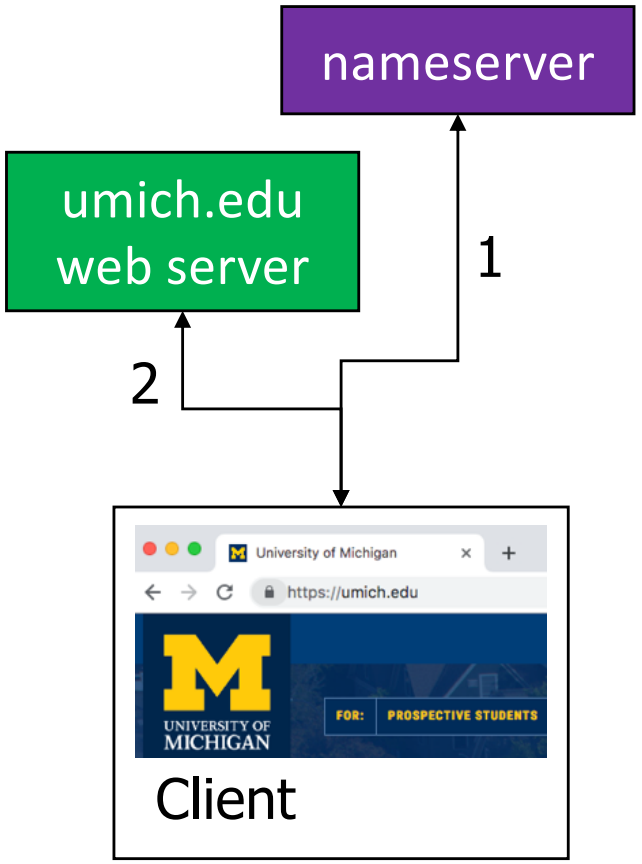
Local nameserver provides IP of **root DNS server**

root DNS server provides IP of **edu DNS server**

edu DNS server provides IP of **umich.edu DNS server**

umich.edu DNS server provides IP of **umich.edu**

Resolution with caching



Local nameserver provides IP of **umich.edu** because it's in the cache

Caching

- There may be a chain of caching DNS servers between client and authority server
  - There's one for CSE
  - Caches DNS requests; answers new requests from cache whenever possible
- Great! But when data changes?
  - Each resource record has time-to-live (TTL) in seconds
  - Counts down from moment authority server emits resource record (RR)
  - Caches and clients must throw out resource records with expired time-to-live

Root nameservers

- Responsible for locating the top level domain name servers (.com, .net, .org, …)
- 13 root name servers in world
  - Their locations are hard-coded in resolving DNS servers
  - Due to caching, involved in few queries

SaaS DNS

- SaaS DNS registration and DNS servers
- AWS Route 53
- Google Cloud DNS
- Microsoft Azure DNS
- Cloudflare DNS

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - Namespace
  - Resolution
  - **Administration**
  - Scaling and security
- Content delivery networks (CDNs)

DNS administration

- IANA (Internet Assigned Numbers Authority) oversees global IP allocation and DNS root zones
- Until 1999, IANA was run by one person, Jon Postel

Jon Postel

- Many contributions to the development of the internet
- Wrote SMTP (email standard)
- In charge of DNS (via IANA)
- "In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior."
- "I think they called me the closest thing to a God of the Internet."

Jon Postel and DNS

- Late 90's, Jon Postel in charge of IANA
- DNS regional root nameservers configured to connect to root zone server managed by US government contractor
- Postel emails admins of 8 root nameservers and tells them to use an IANA server managed by him
- They do it and the US government gets mad

- "I was running a test to see how smoothly a transition could be made."

Jon Postel and DNS

Internet reconfiguration turns out to be rogue

By TED BRIDIS
The Associated Press

WASHINGTON — The Clinton administration said Wednesday it was confident a researcher in California won't repeat his rogue reconfiguration of the Internet — a test that few users noticed but that raised concerns about how the worldwide network is run.

Jon Postel, who runs the Internet Assigned Numbers Authority at the University of Southern California under a Defense Department contract, last week redirected half the Internet's 12 directory-information computers to his own system.

Normally, those so-called "root servers" help users find addresses on the Internet by pulling data from Network Solutions Inc., a private company in northern Virginia that operates under a federal government contract.

Postel, who did not return telephone or e-mail messages, told federal officials afterward he was running a test to see how smoothly such a transition could be made.

Under a plan released last Friday by the administration, the government would end its responsibility of assigning and maintaining Internet addresses and turn the role over to a private, nonprofit organization that doesn't yet exist.

Postel's test "was not, in effect, an attempt to hijack the Net," White House policy adviser Ira Magaziner said Wednesday at a conference of Internet executives.

Magaziner, who described Postel as "a crucial player" in the future of the Internet, said Postel had promised not to repeat the test. But Magaziner also criticized its timing, coming so close to the release of the long-anticipated Internet plan. Groups affiliated with Postel have been critical of the proposal.

"We thought the timing was a bit dicey," Magaziner said. "He said, 'Yeah, that wasn't the right time to do it.' ... I'd give him a bit of slack."

Questions about authorization for such actions can be hard to answer because the Internet still largely operates on an ad-hoc consensus among academics and researchers. Postel gave no prior notification.

"It's caused a good deal of uncertainty and perceived instability in the system," said Chris Clough, a spokesman for Network Solutions, which operates under a contract with the National Science Foundation. "It's a concern about who can authorize changes over the infrastructure and traffic patterns of the Internet."

Officials said the six directory computers still haven't been redirected back to Network Solutions. Becky Burr, associate administrator of the Commerce Department's National Telecommunications and Information Administration, said that was expected to take several more days.

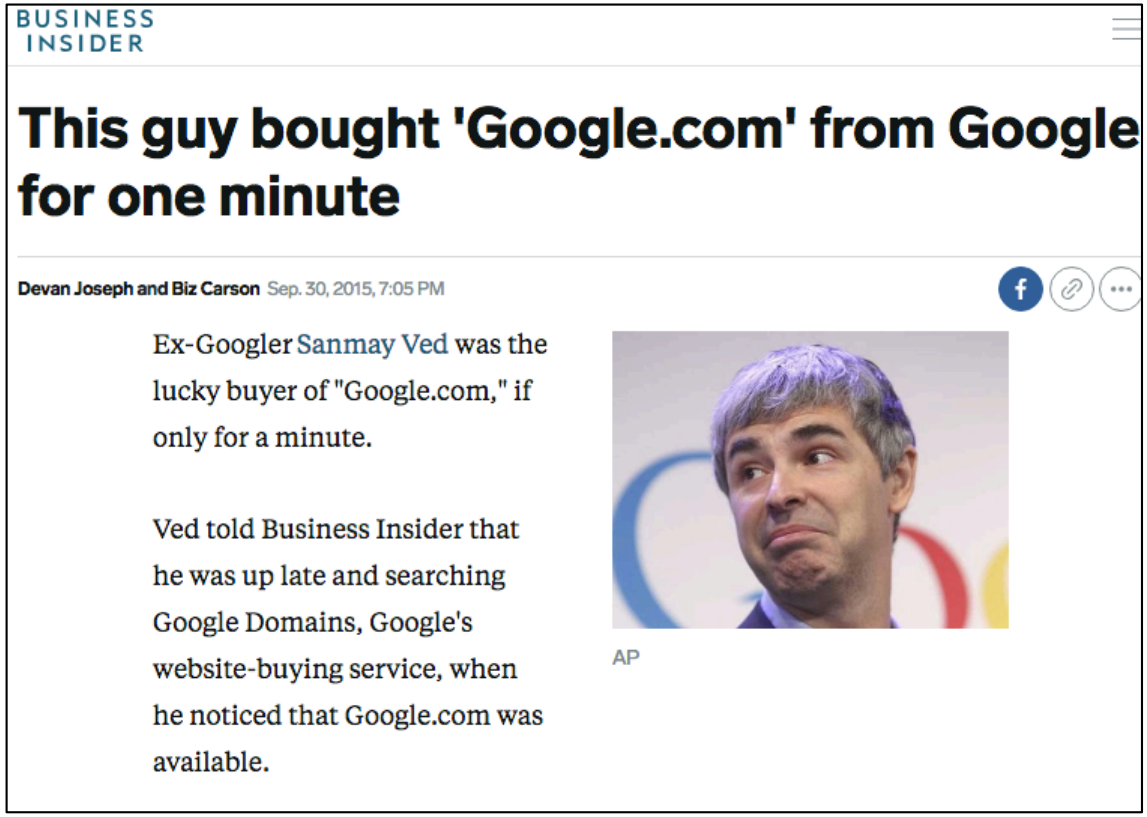
https://news.google.com/newspapers?id=q88aAAAAIBAJ&sjid=1kcEAAAAIBAJ&pg=2900,539368

DNS administration

- Today, IANA is part of the non-profit ICANN
- Administers set of for-profit registrars
  - GoDaddy, NameCheap, Enom, Tucows, etc.
- ICANN under contract with US government
- Much US control of top level DNS

DNS registration

- Domain name registrations have an expiration date
- Google's expired one time. Registrar reversed it.



BUSINESS INSIDER

This guy bought 'Google.com' from Google for one minute

Devan Joseph and Biz Carson Sep. 30, 2015, 7:05 PM

Ex-Googler Sanmay Ved was the lucky buyer of "Google.com," if only for a minute.

Ved told Business Insider that he was up late and searching Google Domains, Google's website-buying service, when he noticed that Google.com was available.

https://www.businessinsider.com/this-guy-bought-googlecom-from-google-for-one-minute-2015-9

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - Namespace
  - Resolution
  - Administration
  - **Scaling and security**
- Content delivery networks (CDNs)

DNS scale

- DNS operates at shocking scale
- Almost every communication starts with a domain name
- What is affected?
  - Personal computers
  - Phones
  - Internet of Things (IoT) devices
  - Backend services
- Example: spam filtering requires 10+ DNS lookups per message!

DNS as a security vulnerability

- DNS is an extreme security vulnerability
- What if someone can remap **`google.com`**?
- What about just denial-of-service?
- Terrorism

DNS cache poisoning

- Bad info is inserted into a DNS server and cached
- Both inadvertent and malicious
- How could one attack CSE's DNS server?

DNS cache poisoning

- DNS cache poisoning is one of the ways that China's Great Firewall works
- Just direct requests to twitter.com to the wrong IP

DNS security remedies

- If you use HTTPS/SSL/TSL, problem mitigated
- DNSSEC is a security extension to DNS
  - Cryptographically signed DNS entries
  - Asymmetric cryptography

Agenda

- Cloud
- Scaling static pages intro
- Domain name system (DNS)
  - Namespace
  - Resolution
  - Administration
  - Scaling and security
- **Content delivery networks (CDNs)**

Scaling static pages solution

- So far, we've talked about how to convert a hostname into the IP address of a server
- How do we return the IP address of a *nearby* server?

Content delivery networks

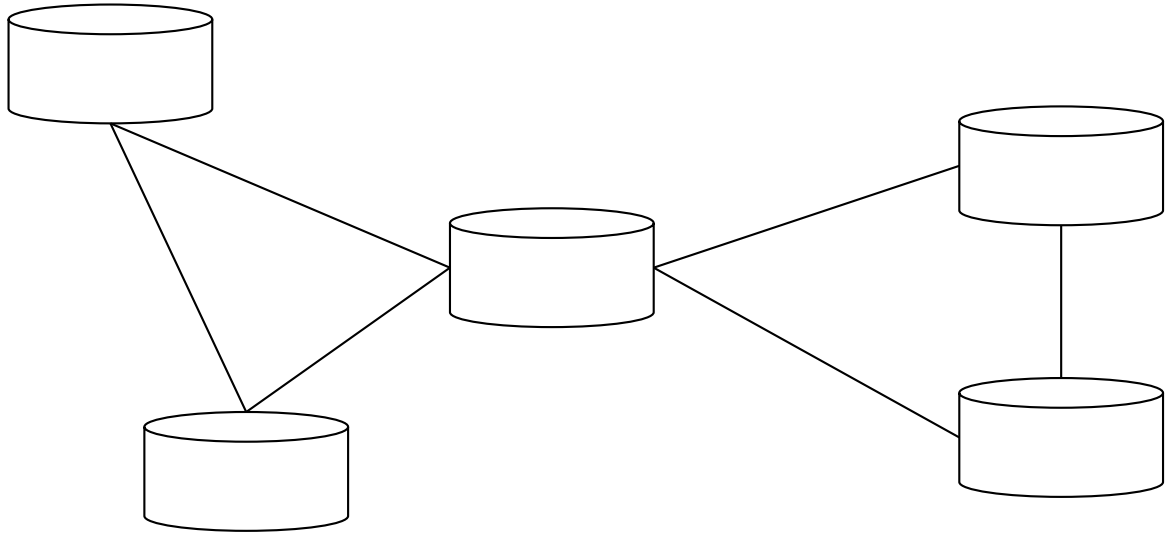
- A content delivery network (CDN) stores static files at many locations throughout the world and serves nearby clients
- Static files: HTML, images, videos
- Large read-only data stored close to client
- Reduce latency to faraway datacenter
- Reduce bandwidth costs by sending data only a short distance

Akamai

- The first content-delivery network
  - You might think the image is from CNN, but Akamai is serving it
  - CNN pays Akamai to do so
- Built on top of a giant DNS hack

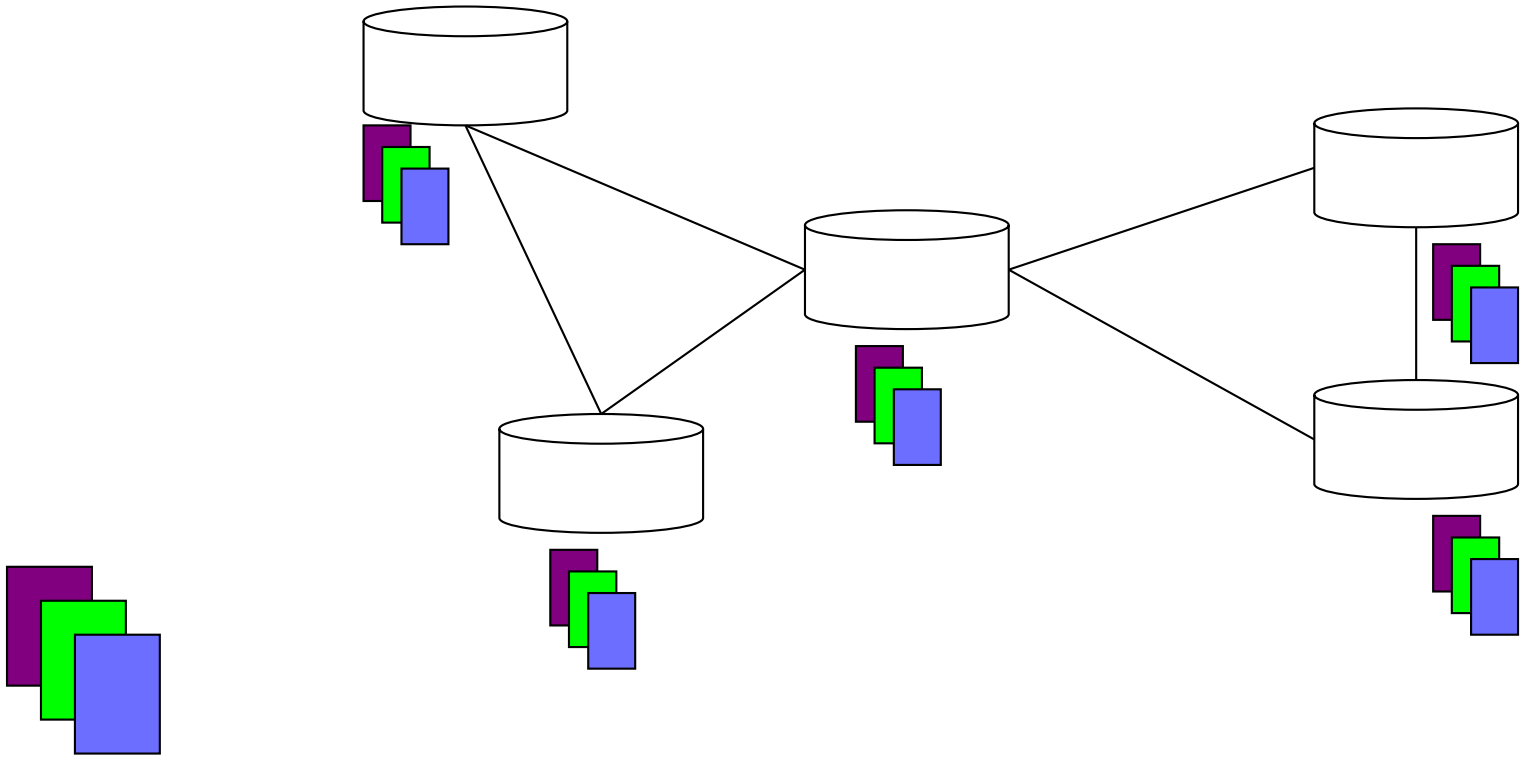
How it works: step 1

- Akamai places servers across country



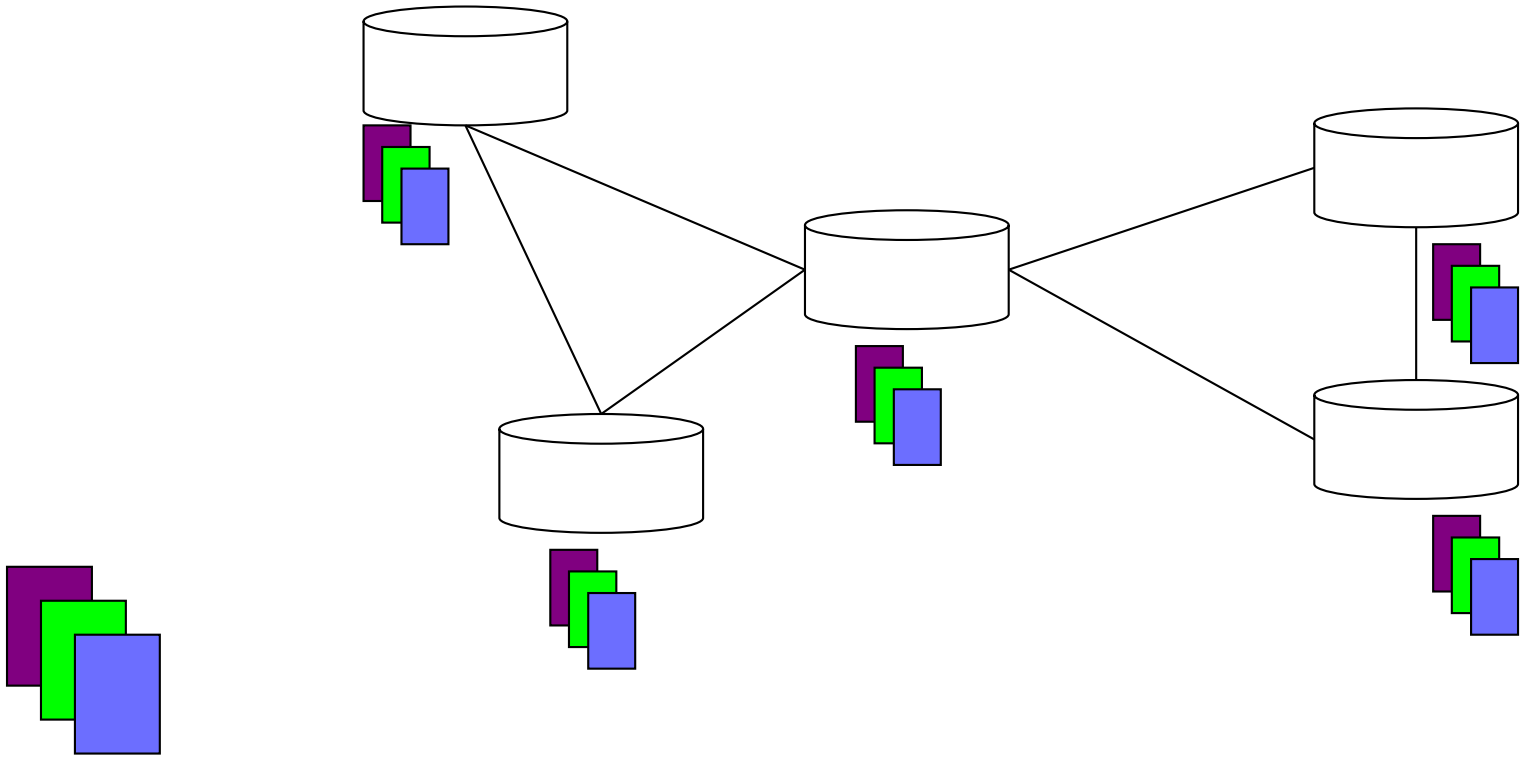
How it works: step 2

- Akamai gets client data
  - Especially images, videos
- Copies to all nodes in network



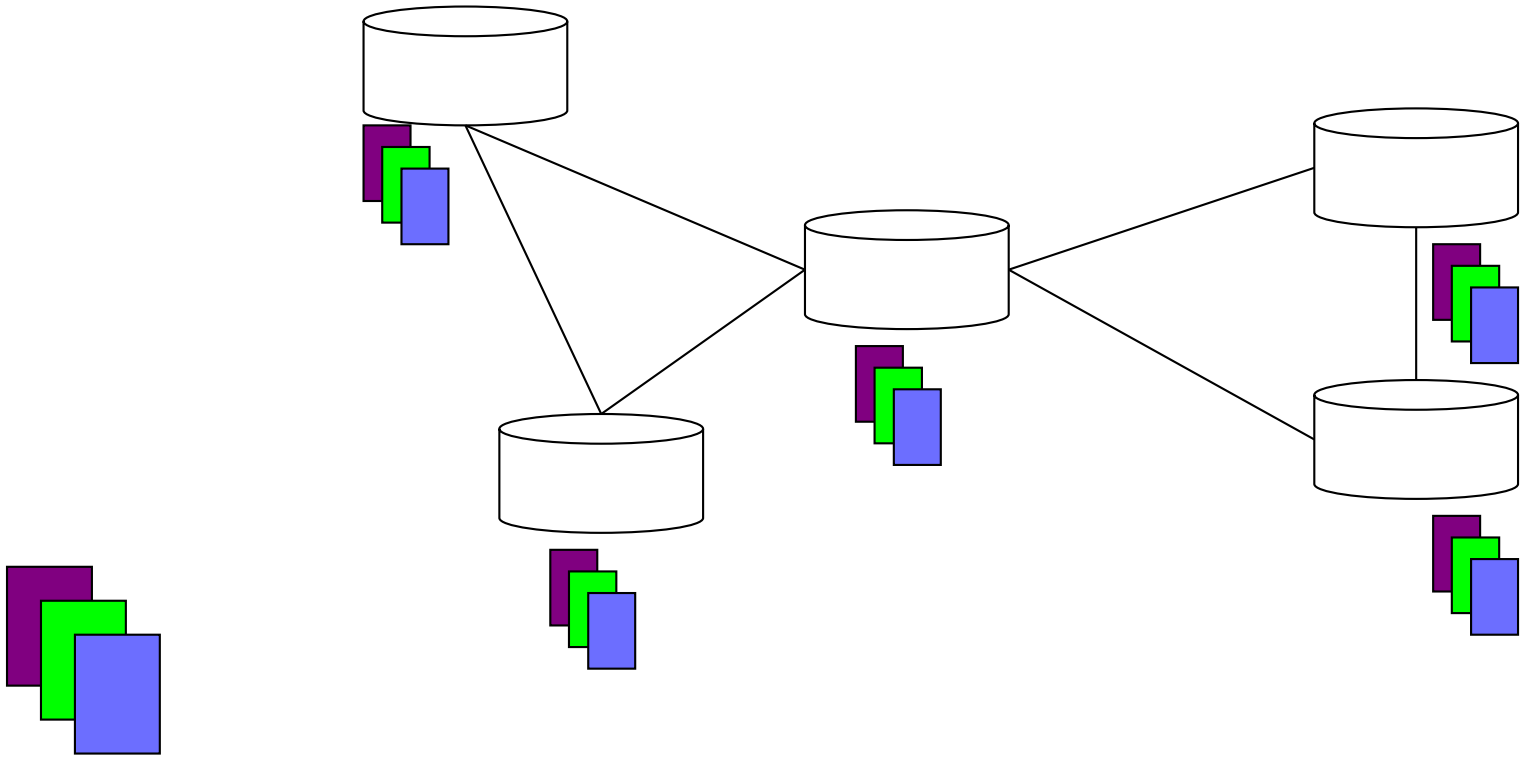
How it works: step 3

- How does client find nearby data?
  - Network conditions can change



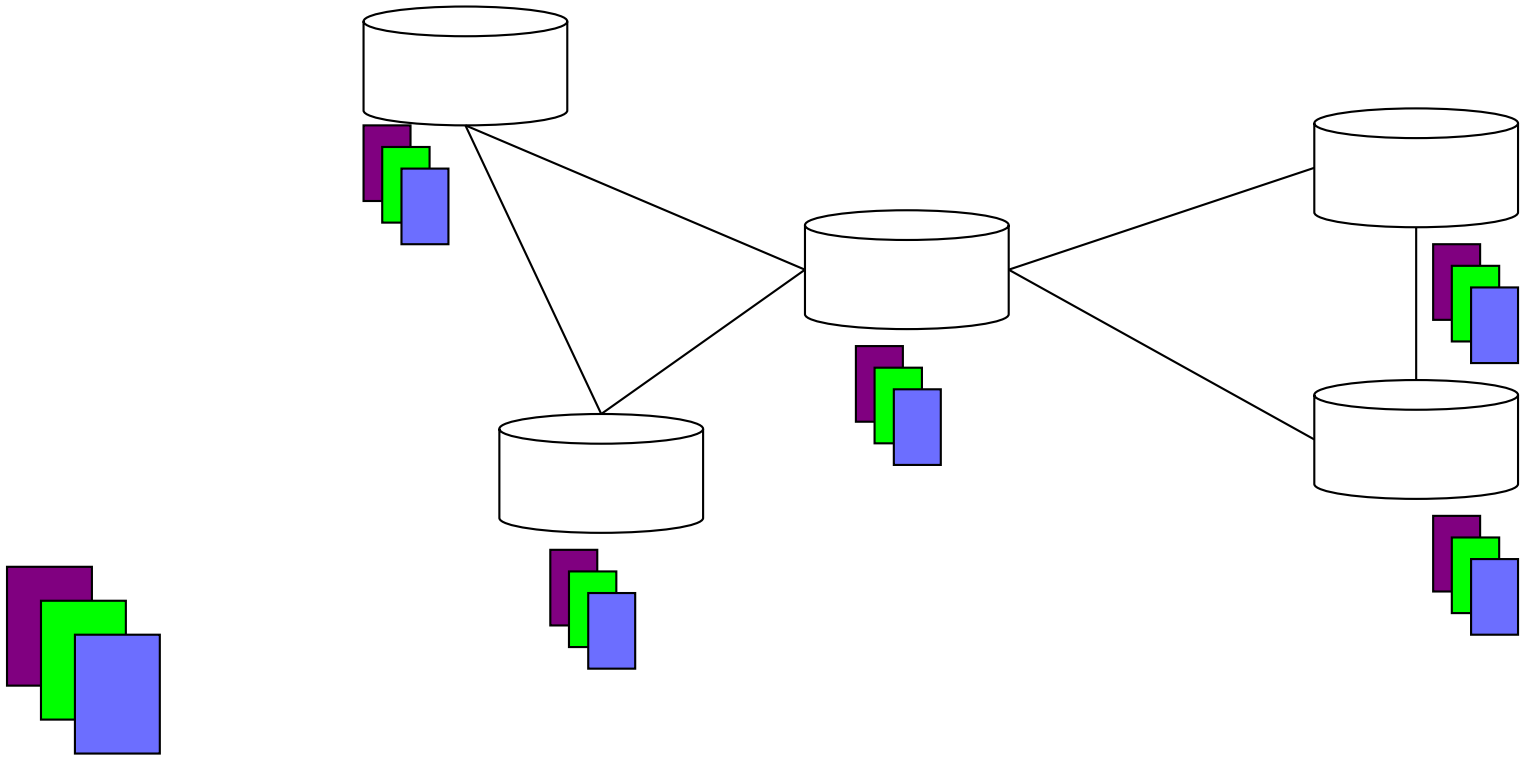
How it works: step 3

- Website rewrites their URLs to uses CDN URLs
  - http://cnn.com/… => http://akadns.akamai.net/….



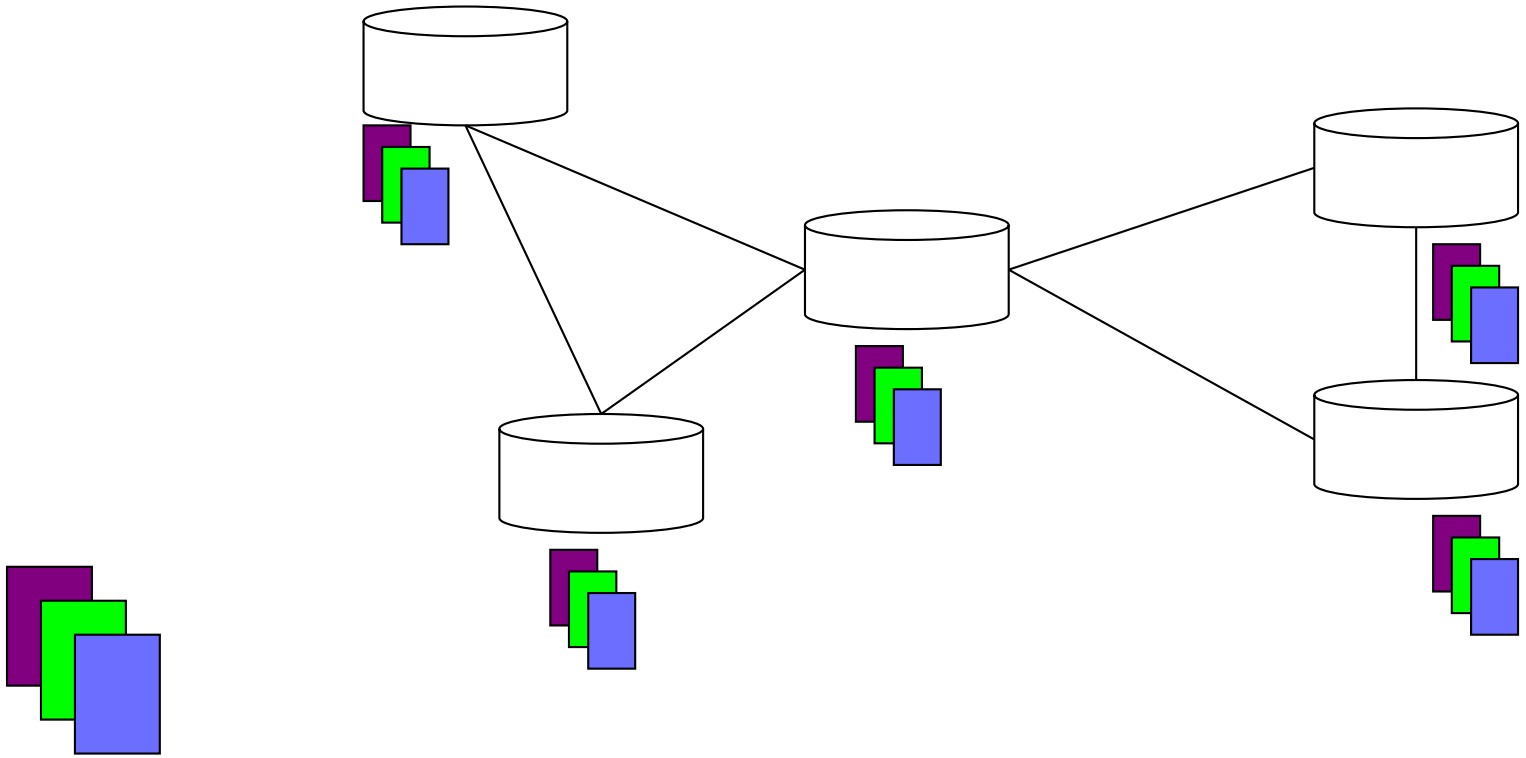
How it works: step 3

- URL contains Akamai-controlled name
  - Specialized Akamai DNS server resolves name to nearby server; tiny TTL



How it works: step 3

- Resolution strongly dependent on
  - Location of client; network conditions; load on Akamai servers; traffic estimation errors



Akamai's scale

- Akmai has 170k servers
- Serves 15%-30% of all web traffic
- What happens if it goes down?

CDN outtages

- When CDN goes down, website goes down!

Our CDN was unable to reach our servers

Please check www.redditstatus.com if you consistently get this error.

PaaS CDN

- CDN availble via PaaS
  - Rent a CDN
- AWS Cloud Front
- Google Cloud CDN
- Microsoft Azure CDN
- Cloudflare CDN

CDN recap

- Custom DNS servers dynamically direct clients to best caching servers
- Static content
- Reduces latency for clients fetching content
- Reduces load on datacenter servers

Summary

- Today: scaling static pages
  - Domain name server (DNS) resolves a domain name to an IP address
  - Content delivery networks (CDN) scale static content delivery using modified DNS
- Next time: scaling dynamic content