The Domain Name Service, Etc.

Jeff Chase
Duke University, Department of Computer Science
CPS 212: Distributed Information Systems

1. Domain Name Service (DNS) illustrates:
   - issues and structure for large-scale naming systems
   - use of hierarchy for scalability
   - decentralized administration of the name space
   - hierarchical authority and trust

2. Role of DNS in wide-area request routing
   - DNS round robin
   - Content Distribution Networks: Akamai, Digital Island

DNS 101

Domain names are the basis for the Web’s global URL space. Provides a symbolic veneer over the IP address space. Names for autonomous naming domains, e.g., cs.duke.edu names for specific nodes, e.g., fran.cs.duke.edu names for service aliases (e.g., www, mail servers)

- Almost every Internet application uses domain names when it establishes a connection to another host.

The Domain Name System (DNS) is a planetary name service that translates Internet domain names.

maps <node name> to <IP address> (mostly) independent of location, routing etc.

Domain Name Hierarchy

DNS name space is hierarchical:
- fully qualified names are “little endian”
- scalability
- decentralized administration
- domains are naming contexts replaces primordial flat hosts.txt namespace

DNS Implementation 101

DNS protocol/implementation:
- UDP-based client/server
- client-side resolvers typically in a library gethostbyname, gethostbyaddr
- cooperating servers query-answer-referral model forward queries among servers server-to-server may use TCP ("zone transfers")
- common implementation: BIND

DNS Name Server Hierarchy

DNS servers are organized into a hierarchy that mirrors the name space. Specific servers are designated as authoritative for portions of the name space.

Servers may delegate management of subdomains to child name servers.
Parents refer subdomain queries to their children.

Root servers list servers for every TLD.
Subdomains correspond to organizational (administrative) boundaries, which are not necessarily geographical.
Servers are bootstrapped with pointers to selected peer and parent servers.
Results are bootstrapped with pointers to root or more local servers, they make recursive queries.
DNS: The Politics

He who controls DNS controls the Internet.

- TLD registry run by Network Solutions, Inc. until 9/98.
  - US government (NSF) granted monopoly, regulated but not answerable to any US or international authority.
- Registration is transitioning to a more open management structure involving an alphabet soup of organizations.

For companies, domain name == brand.

- Squatters register/resell valuable domain name “real estate”.
- Who has the right to register/use, e.g., coca-cola.com?

DNS: The Big Issues

1. Naming contexts
   I want to use short, unqualified names like whiteout instead of whiteout.cs.duke.edu when I’m in the cs.duke.edu domain.

2. What about trust? How can we know if a server is authoritative, or just an impostor?
   - What happens if a server lies or behaves erratically? What denial-of-service attacks are possible? What about privacy?

3. What if an “upstream” server fails?

4. Is the hierarchical structure sufficient for scalability?
   - more names vs. higher request rates

DNS Caching

Caching of query responses allows subsequent queries to bypass the roots of the server hierarchy.

Each response is stamped with a time-to-live (TTL) to limit damage from stale cache entries.

What about negative caching: is it worthwhile to cache negative responses?

DNS Replication

Every DNS domain has or should have at least one secondary name server replica.

- configure peers to offload queries from primary
- serve as authoritative backup

Secondary replicas keep themselves up to date by periodically fetching/refreshing the entire naming database via zone transfer (TCP).

The primary database is timestamped with a “serial number” to short-circuit if no updates have occurred since last zone transfer.

How to load-balance the secondaries?

What if primary is overloaded with too many secondary requests requesting zone transfers?

Reverse Translation

152

3

4...

40

The Server Selection Problem

Which server?

Which network site?

“Contact the weather service.”
DNS Round Robin

What about DNS caching?
How to handle server failures?
How effective is the load balancing?

Cisco DistributedDirector uses a more sophisticated DNS load balancing approach, based on its Director Response Protocol (DRP), and also incorporates HTTP redirection.

DNS-based Request Routing

How to apply the request routing function $f$?
• Some intermediary intercepts the request, and directs it to a selected site. Smart proxies or switches? E.g., look at URL or server IP address.
• Or, interpose on the binding procedure, before the client sends the request itself. Smart clients, Active Names, RPC binding, or DNS lookup.

Third-party CDNs are based on DNS servers that select the cache/replica site on DNS lookup for the request. Akamai, Digital Island, Web hosting providers (e.g., Exodus), etc. Like DNS-RR… but smarter…

Domain Granularity and “Akamaizing”

• CDN (e.g., Akamai) creates new domain names for each client content provider. e.g., a128.g.akamai.net.
• The CDN’s DNS servers are authoritative for the new domains.
• The client content provider modifies its content so that embedded URLs reference the new domains. “Akamaize” content, e.g., http://www.cnn.com/image-of-the-day.gif becomes http://a128.g.akamai.net/image-of-the-day.gif.
• Using multiple domain names for each client allows the CDN to further subdivide the content into groups.

Using DNS for Third-party CDNs

Intelligent DNS-based request routing has some tricky parts:
• Third-party CDNs contract with content providers (e.g., Web sites such as cnn.com) to serve a subset of their content. Resource-rich content, e.g., images, audio, video.
• To use DNS request routing, the CDN must assume DNS duties for the URLs that reference the content it serves.
• The content provider does not want to designate the CDN as the authoritative DNS server for its domain (e.g., cnn.com).

Solution: make up new DNS domains for the client provider’s content served by the CDN.
The Akamai et. al. DNS Hook

get

http://www.nhc.noaa.gov

a

DNS server for
nhc.noaa.gov

b

c

local

DNS server

local

DNS server

“Akamaizes” its content.

“Akamaized” response object has inline URLs for secondary content at a128.g.akamai.net and other Akamai-managed DNS names.

Wide-Area Request Routing

What information does a DNS-based request routing function $f$ have available to it?

- client’s or proxy’s DNS resolver’s IP address
  - Gives the best guess at where the client is...can we do better?
- domain name embedded in URL content domain
- NOT the rest of the URL
- other information about server load or network state

The CDN decides where to cache/replicate each content domain, and which cache/replica to serve each request.

Directory Services (e.g., LDAP)

A directory service is a souped-up name service.

- read-mostly access to named entries with unique, global distinguished names
- clients see a uniform view of a hierarchical name space authority to serve the name space is partitioned across a collection of servers partitioning reflects geographical or organizational boundaries context-based lookups with referrals
- simple updates: add/delete/update single entry
- large-scale caching/replication with soft consistency

Attributes and Searching

Directory services are augmented with support for attributes.

- An entry is a named collection of attributes.
- An attribute is a typed collection of values, whose format is defined by its type.
  - e.g., printer, name=buzzard, location=LSRC 312, resolution=600dpi
- Attributes are more useful if their types are standardized

Attributes can be used as the basis for searches that find an object with specified properties.

- can specify filters, scope of search, etc.
- goal: attribute-based definition of services