IT 609
Network and System Administration

Domain Name Server (DNS)

Tuesday November 02, 2021

Domain Name Server (DNS)

DNS - Domain Name Server

When the Internet was small, each host had `hosts.txt` file to map names to IP's

DNS developed to resolve names as Internet grew

Consists of Name Server, Database, and Name Resolver

DNS is both distributed and hierarchical

Each server is responsible for one or more zones

Each zone should have two or more servers (1 primary, 1+ secondary)

Root DNS Servers

13 Root Servers, named A thru M provide the foundation for the DNS system

Top Level Domains

.gov - government

.mil - military

.int - international organizations

.edu - educational

.com - commercial

.org - non-profit and other organizations

.net - networks and telecom organizations

Also two-letter country codes for non-US countries

E.g., .jp, .de, .ru, .ca, .uk, .it, .ch

Top Level Domain Changes

2000-2002 Additions

.aero, .biz, .coop, .info, .museum, .name, .pro

2003 Additions

.asia, .cat, .jobs, .mobi, .tel, .travel

2010 Additions

Internationalized TLDs

2011 Addition

.xxx

2012 Addition

Generic TLDs (gTDL)

Top Level Domains

The Root Servers know of the individual servers that take care of each of the top level domains

TLD's are managed by different Registries

Each Registry must maintain the listing of all groups, companies, organizations, etc in that TLD

Registries may sell the domain names directly or may contract that service out to other companies

e.g. VeriSign is the Registrar for .com, .name, and .net, but you can buy a .com name from multiple ISP's

DNS as Abstractions

Names allow IP addresses to be hidden - this is a good thing!

- IP addresses can change or move while the name remains
- Names might resolve to multiple IP addresses
- IP addresses might be outside of an organization's normal space (e.g. mycourses.unh.edu)
- Multiple names (including different TLDs) can be assigned to the same IP

DNS also includes aliases (CNAME) for additional abstractions

Name Resolution

Clients only talk to their local name server

Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn

Name Resolution

Clients only talk to their local name server

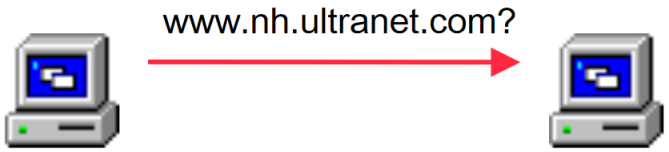
Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn

Name Resolution

Clients only talk to their local name server

Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn

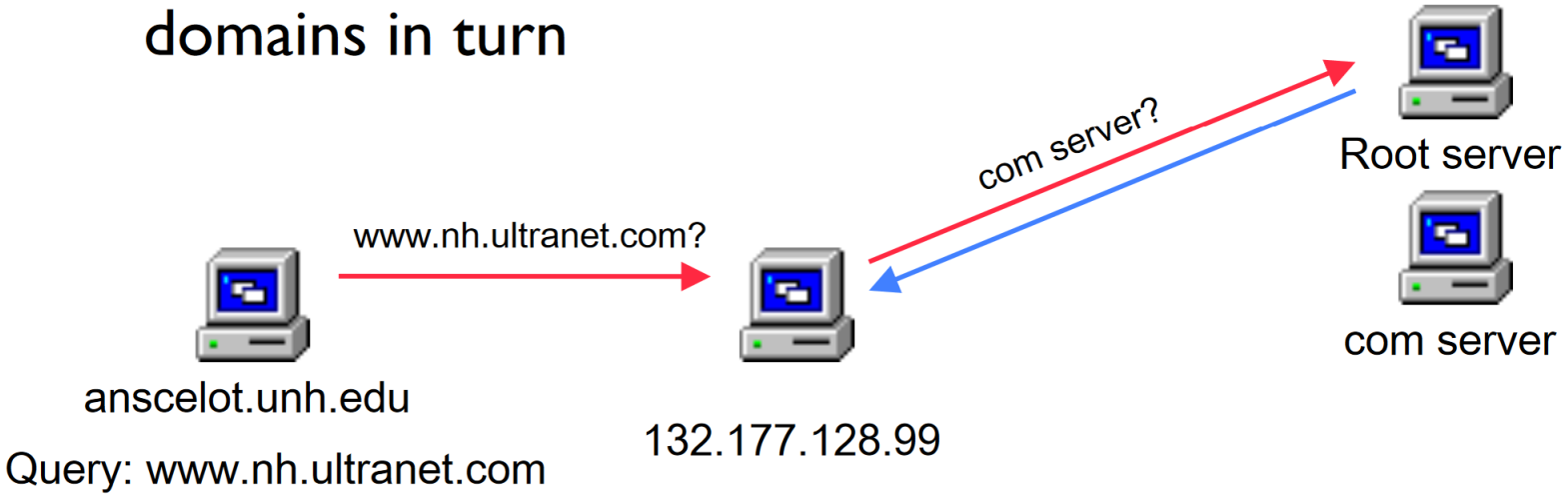
Root server



Name Resolution

Clients only talk to their local name server

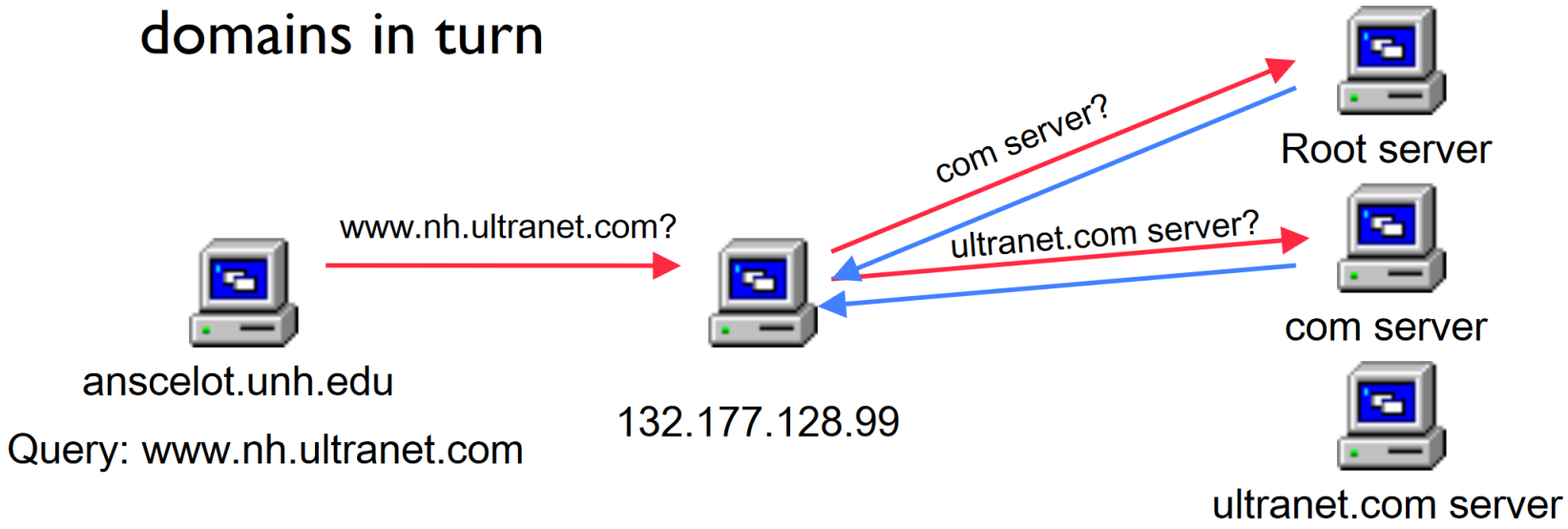
Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn



Name Resolution

Clients only talk to their local name server

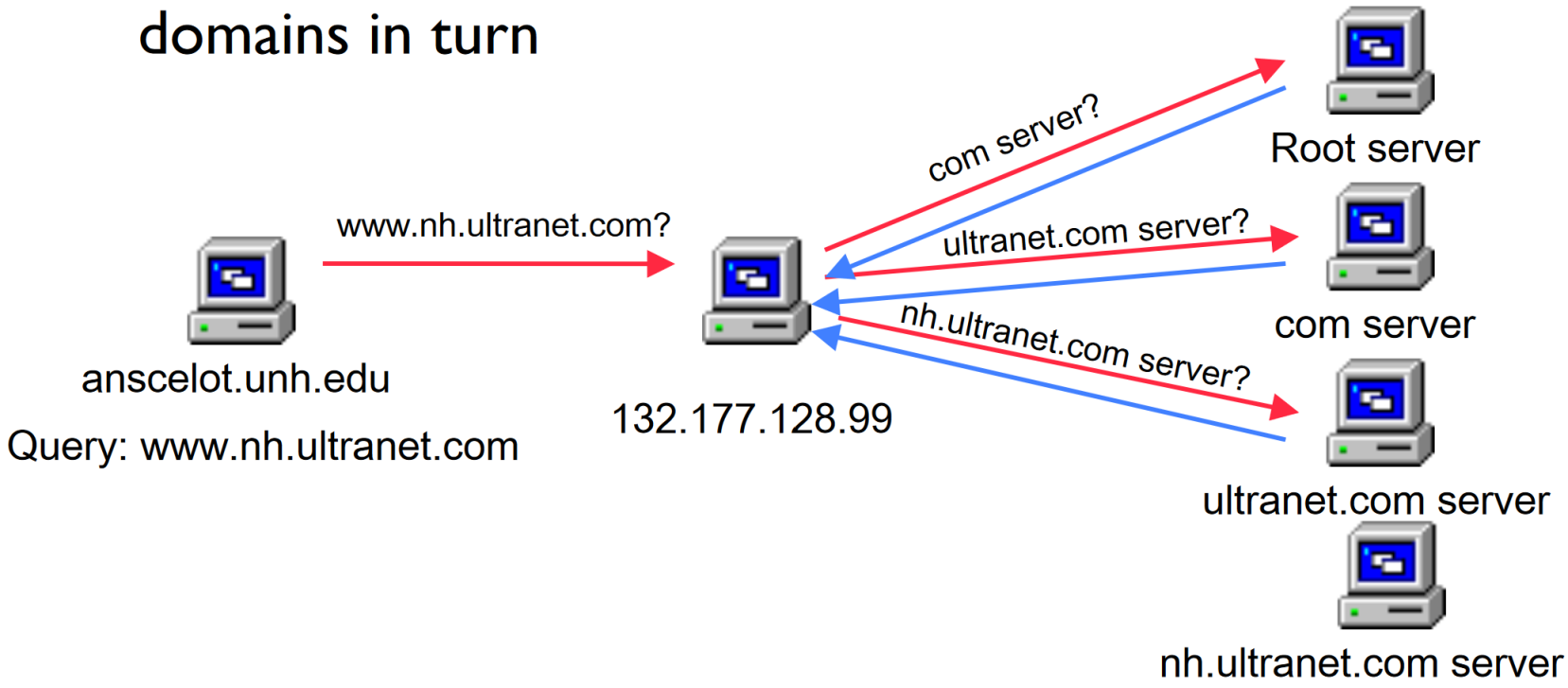
Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn



Name Resolution

Clients only talk to their local name server

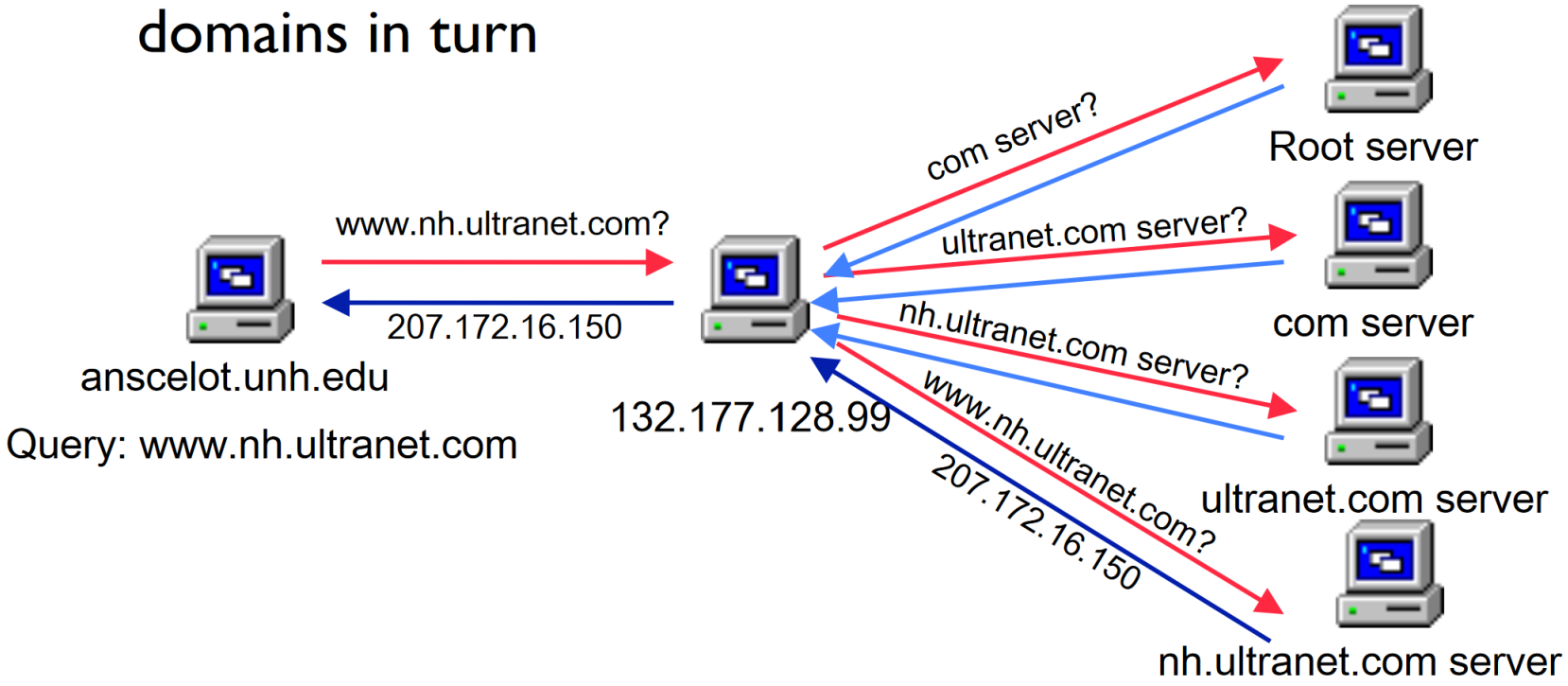
Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn



Name Resolution

Clients only talk to their local name server

Non-local requests are referred by the server to the root servers and to specific servers for the domains in turn



Local DNS Servers and Database

Primary servers contain DNS information based on manually configured files

Secondary servers get their info from the primary servers

Servers also cache resolved names temporarily for efficiency purposes

The database records can contain:

- Name to IP mappings
- IP to Name mappings
- Info on DNS structure
- Info on services available on local servers

Record Types

A - IP address for a given name

AAAA - IPv6 address for a given name

PTR - name for a given IP address

CNAME - aliases

HINFO - host information

MX - mail exchange records

SOA - statement of authority for a zone

NS - name servers for a zone

SRV - service location records

…and more: https://en.wikipedia.org/wiki/List_of_DNS_record_types

Sample DNS Database

```
it609.com.      IN SOA  ns1.it609.com. (
                        djb1.it609.com.
                     2011101702   ; serial #
                          10800   ; refresh (3 hours)
                           3600   ; retry (1 hour)
                         604800   ; expire (1 week)
                          86400)  ; TTL (1 day)
it609.com.      IN NS ns1.it609.com.
                IN NS ns2.it609.com.
it609.com.      IN MX   20  pony
                IN MX   40  express
ns1             IN A  192.168.100.5
                 IN A  192.168.150.17
ns2             IN A  192.168.200.5
pony            IN A  192.168.101.2
express         IN A  192.168.102.8
mail            IN CNAME pony
```

Dynamic DNS

Designed for use with DHCP

Hosts can register themselves with the DNS server to indicate what machine name matches what IP address

Can also dynamically create service records

Very important for Windows Server and Active Directory

Can open some security concerns as anyone can select any machine name and get it registered in DNS

DNS Security

DNS was not designed with security in mind

Current issues

- DNS spoofing
- DNS cache poisoning
- DNS ID hacking

DNSSEC is solution to mitigate risks that is being implemented

- DNSSEC signs DNS records so that they can be trusted as valid
- First root-level deployment in June 2010