The Domain Name System

History of DNS

- Before DNS
  - ARPAnet
    - *HOSTS.txt* contains all the hosts' information
    - Maintained by SRI's Network Information Center
      - In SRI-NIC host
  - Problems: Not scalable!
    - Traffic and Load
    - Name Collision
    - Consistency
- Domain Name System
  - Administration decentralization
  - 1984
    - Paul Mockapetris (University of Southern California)
    - RFC 882, 883 → 1034, 1035
      - 1034: Concepts
      - 1035: Implementation and Specification

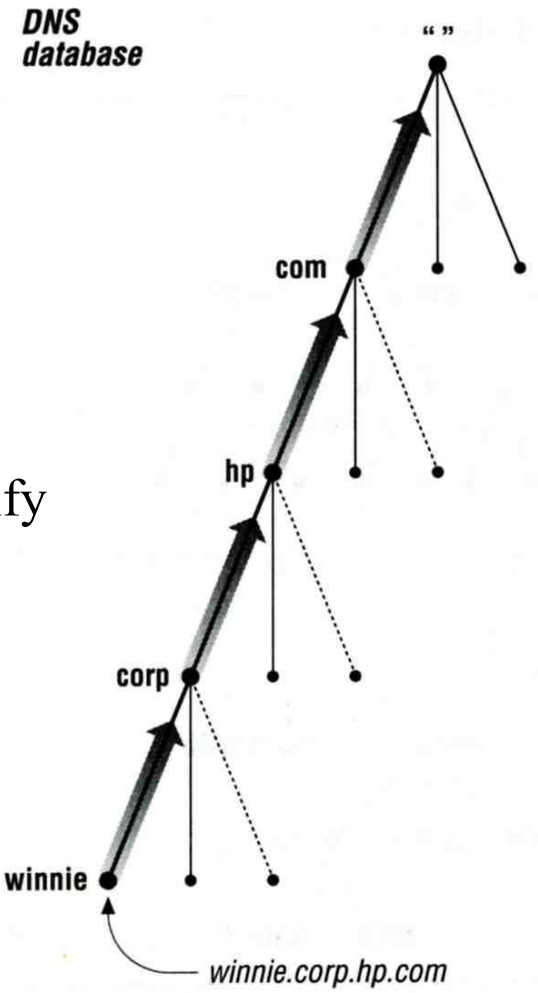
RFC Sourcebook:
http://www.networksorcery.com/enp/default0304.htm

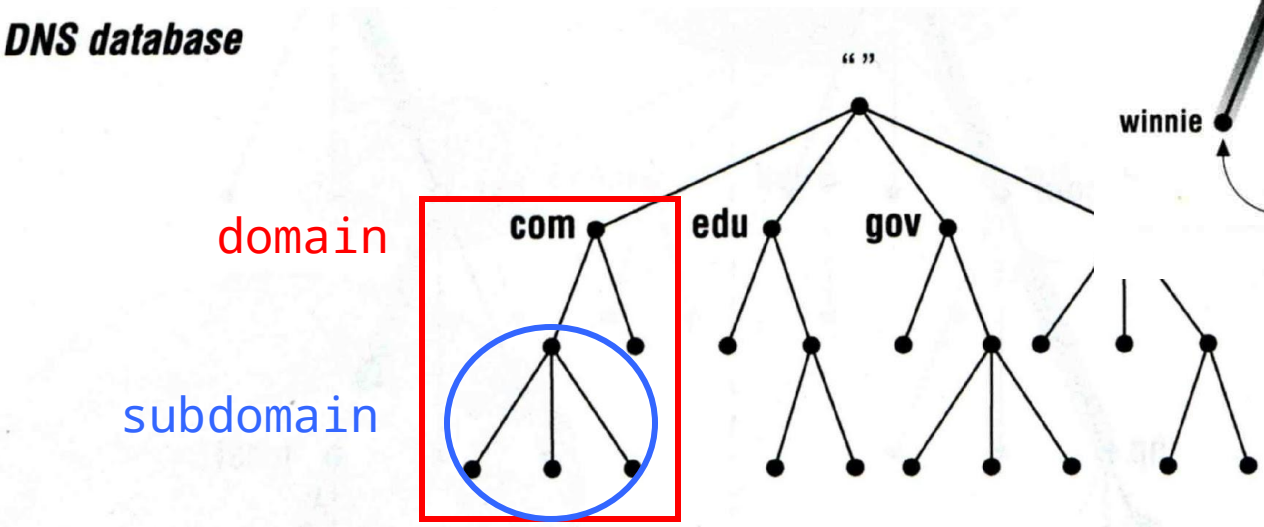
DNS Introduction – DNS Specification

- Make domain name system as
  - Tree architecture
    - Each subtree ➔ "***domain***"
    - Domain can be divided in to "***subdomain***"
  - Distributed database
    - Each site maintains segment of DB
    - Each site open self information via network
  - Client-Server architecture
    - Name servers provide information (Name Server)
    - Clients make queries to server (Resolver)

DNS Introduction – Domain and Subdomain

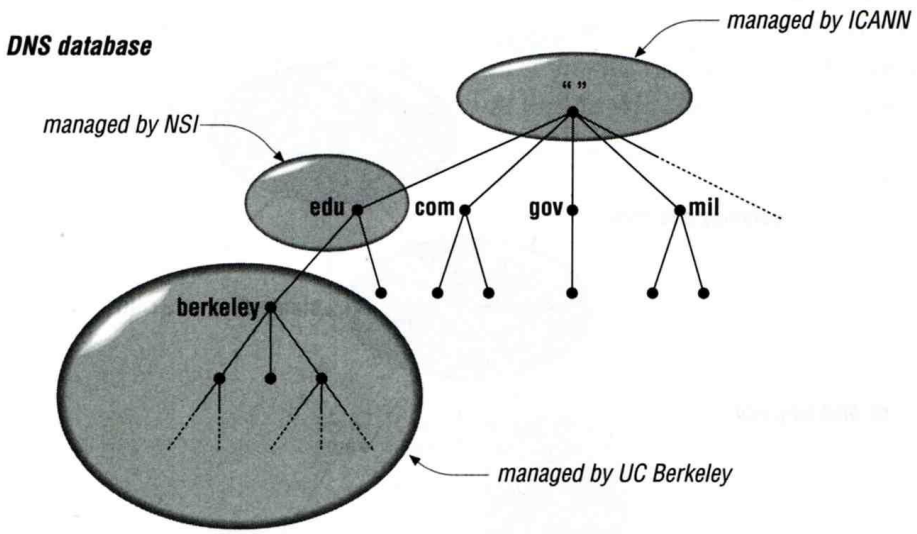
- DNS Namespace
  - A tree of domains
- Domain and subdomain
  - Each domain has a "domain name" to identify its position in database
    - EX: nctu.edu.tw
    - EX: cs.nctu.edu.tw





The DNS Namespace (1)

- A inverted tree (Rooted tree)
  - Root with label "."
- Domain level
  - Top-level or First level
    - Child of the root
  - Second-level
    - Child of a First-level domain
- Domain name limitation
  - 63-characters in each component and
  - Up to 255-characters in a complete name



The DNS Namespace (2)

- gTLDs
  - generic Top-Level Domains, including:
  - com: commercial organization, such as ibm.com
  - edu: educational organization, such as purdue.edu
  - gov: government organization, such as nasa.gov
  - mil: military organization, such as navy.mil
  - net: network infrastructure providing organization, such as hinet.net
  - org: noncommercial organization, such as x11.org
  - int: International organization, such as nato.int

ICANN – Internet Corporation for Assigned Names and Numbers
http://www.icann.org/

The DNS Namespace (3)

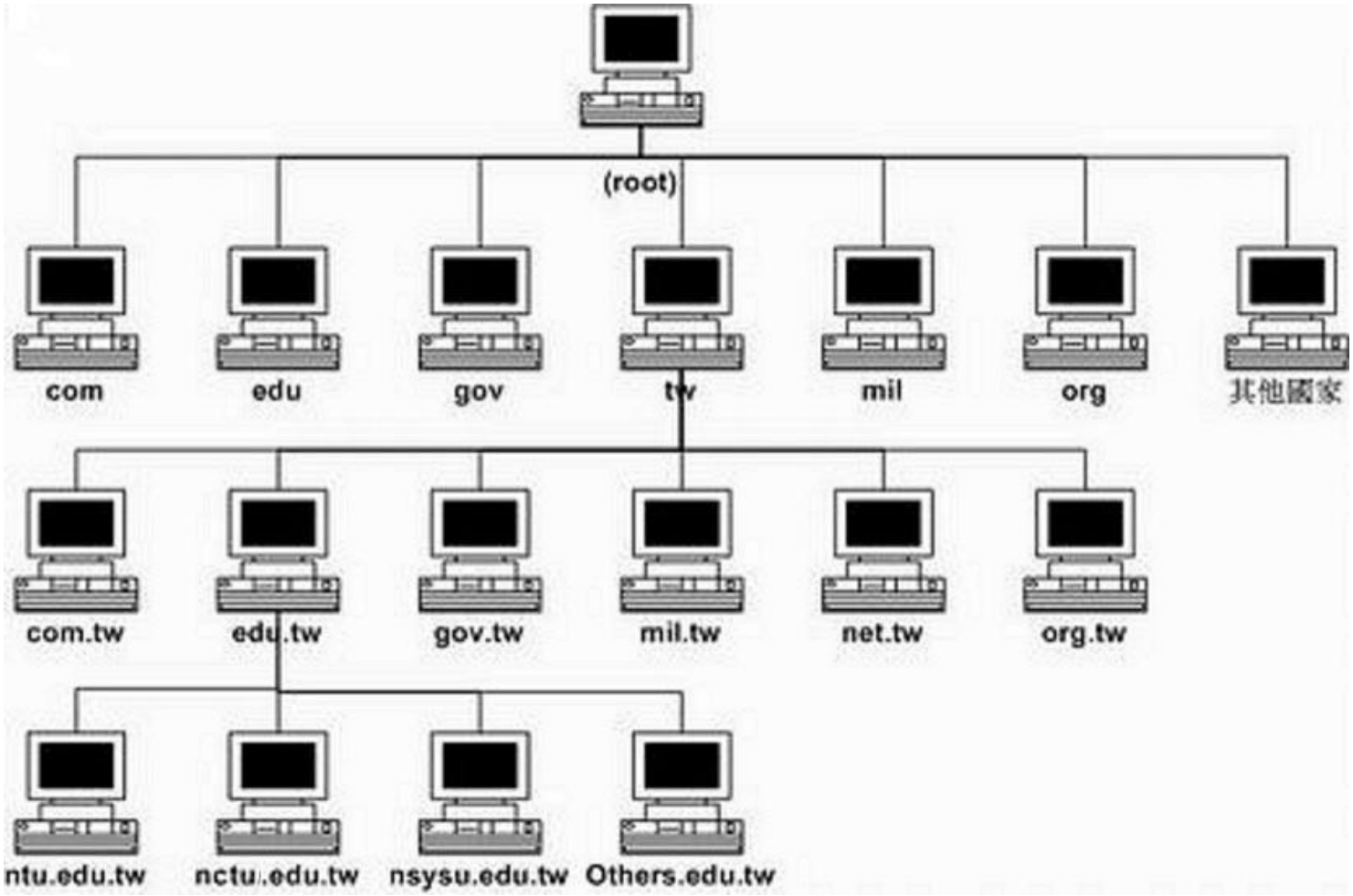
- New gTLDs launched in year 2000:
  - aero: for air-transport industry
  - biz: for business
  - coop: for cooperatives
  - info: for all uses
  - museum: for museum
  - name: for individuals
  - pro: for professionals

REF: http://data.iana.org/TLD/tlds-alpha-by-domain.txt

The DNS Namespace (4)

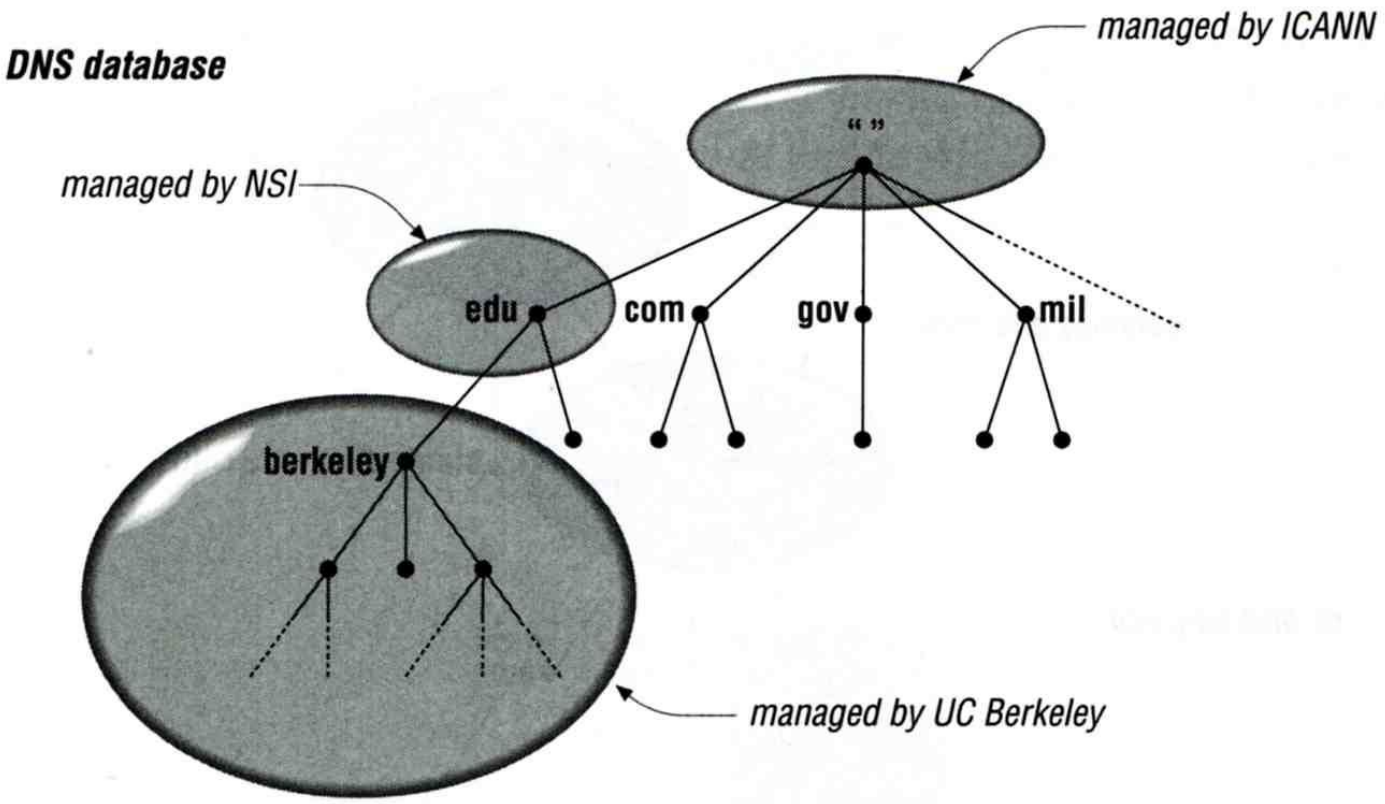
- Other than US, ccTLD
  - country code TLD (ISO 3166)
    - Taiwan → tw
    - Japan → jp
  - Follow or not follow US-like scheme
    - US-like scheme example
      - edu.tw, com.tw, gov.tw
    - Other scheme
      - co.jp, ac.jp

DNS Namespace (5)



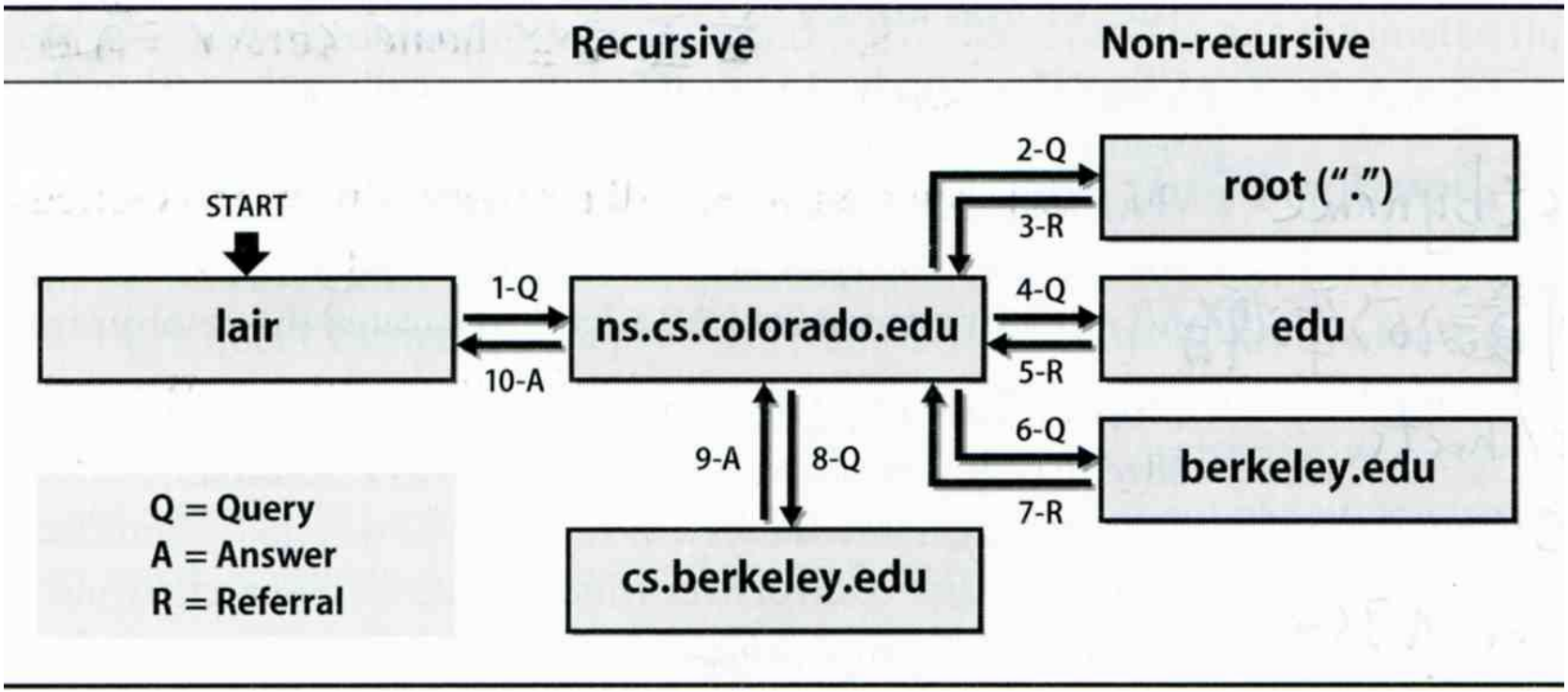
How DNS Works – DNS Delegation

- Administration delegation
  - Each domain can delegate responsibility to subdomain



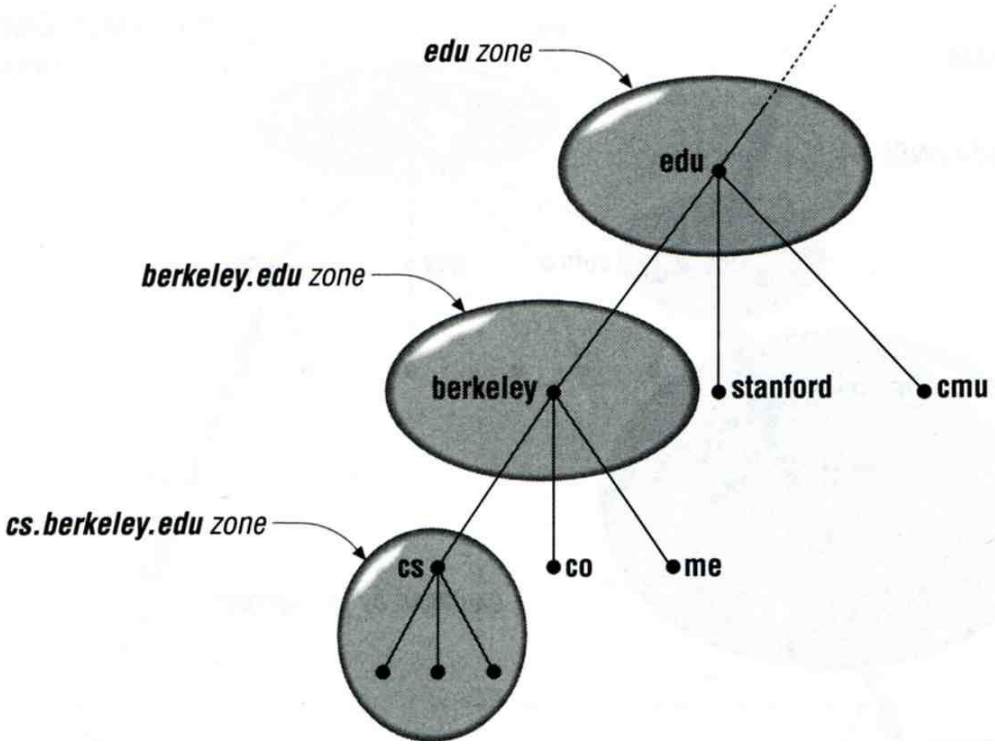
How DNS Works – DNS query process

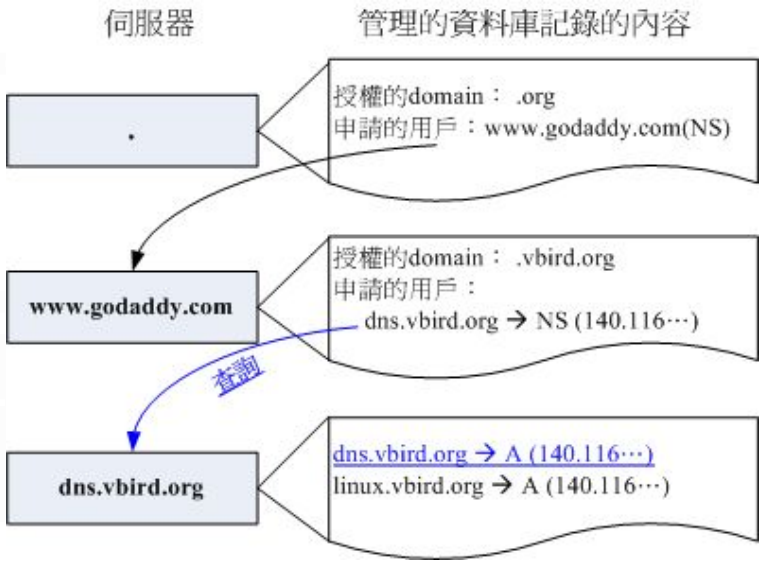
- Recursive query process
  - Ex: query lair.cs.colorado.edu → vangogh.cs.berkeley.edu, name server "ns.cs.colorado.edu" has no cache data



DNS Delegation – Administrated Zone

- Zone
  - Autonomously administered piece of namespace
    - ➢ Once the subdomain becomes a zone, it is independent to it's parent
      - – Even parent contains NS's A record





DNS Delegation – Administrated Zone

- Zone
  - Autonomously administered piece of namespace
- Two kinds of zone files
  - Forward Zone files
    - Hostname-to-Address mapping
    - Ex:
      - bsd1 IN A 140.113.235.131
  - Reverse Zone files
    - Address-to-Hostname mapping
    - Ex:
      - 131.235.113.140 IN PTR bsd1.cs.nctu.edu.tw.
  - Forward zone is necessary

The Name Server Taxonomy (1)

- Categories of name servers
  - Based on a name server's source of data
    - Authoritative: official representative of a zone
      - Master: get zone data from disk
      - Slave: copy zone data from master
    - Nonauthoritative: answer a query from cache
      - caching: cashes data from previous queries
  - Based on the type of data saved
    - Stub: a slave that copy only name server data (no host data)
  - Based on the type of answers handed out
    - Recursive: do query for you until it return an answer or error
    - Nonrecursive: refer you to the authoritative server
  - Based on the query path
    - Forwarder: performs queries on behalf of many clients with large cache

The Name Server Taxonomy (2)

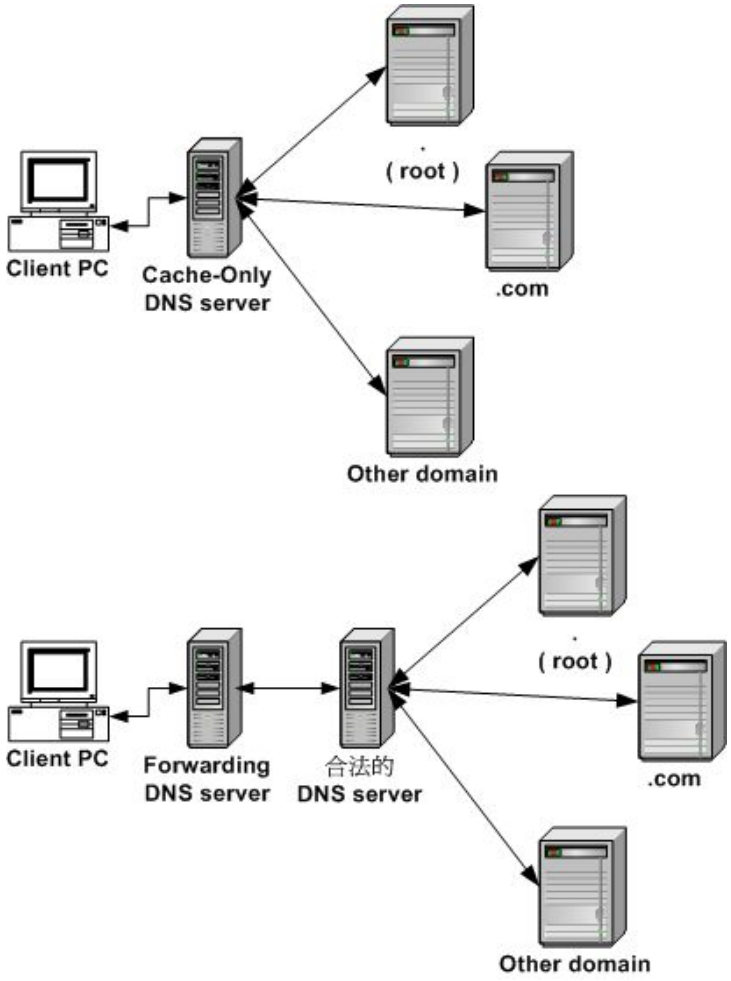
- Nonrecursive referral
  - Hierarchical and longest known domain referral with cache data of other zone's name servers' addresses
  - Ex:
    - Query lair.cs.colorado.edu from a nonrecursive server
    - Whether cache has
      - Name servers of cs.colorado.edu, colorado.edu, edu, root
  - The resolver libraries do not understand referrals mostly. They expect the local name server to be recursive

The Name Server Taxonomy (3)

- Caching
  - Positive cache
  - Negative cache
    - No host or domain matches the name queried
    - The type of data requested does not exist for this host
    - The server to ask is not responding
    - The server is unreachable of network problem
- Negative cache
  - 60% DNS queries are failed
  - To reduce the load of root servers, the authoritative negative answers must be cached

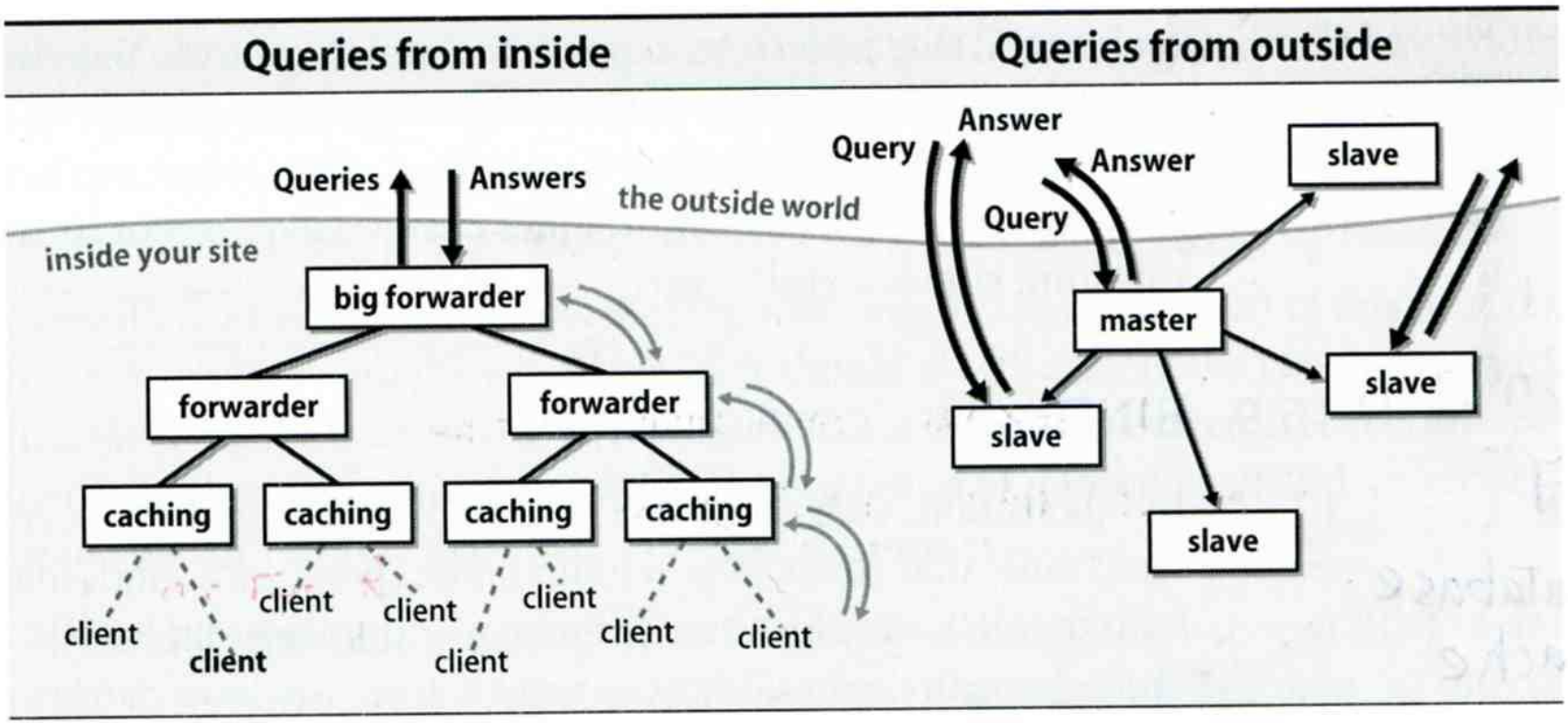
The Name Server Taxonomy (4)

- Caching and forwarder DNS server



The Name Server Taxonomy (5)

- How to arrange your DNS servers?
  - Ex:



The Name Server Taxonomy (6)

- Root name servers
  - List in named.root file of BIND

```
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
```

DNS Client

- /etc/resolv.conf
  - nameserver, domain, search
- /etc/hosts
- /etc/nsswitch.conf

DNS Database

The DNS Database

- A set of text files such that (RFC 1035)
  - Maintained and stored on the domain's master name server
  - Types of entries
    - Comments(;)
    - Resource Records (RR)
      - Used to store the information of
      - The real part of DNS database
    - Directives
      - Used to process content of a zone file

The DNS Database – Directives

- Directives start with a dollar sign($), must start in first field and be on a line by themselves

- $ORIGIN domain-name
  - Used to append to un-fully-qualified name
- $INCLUDE file-name
  - Separate logical pieces of a zone file
  - Keep cryptographic keys with restricted permissions
- $TTL default-ttl
  - Default value for time-to-live filed of records
- $GENERATE start-stop/[step] lhs type rhs (BIND only)
  - Used to generate a series of similar records
  - Can be used in only CNAME, PTR, NS record types

The DNS Database – Resource Record (1)

- Basic format
  - [name] [ttl] [class] type data
    - name: the entity that the RR describes
      - Can be relative or absolute
    - ttl: time in second of this RR's validity in cache
    - class: network type
      - IN for Internet
      - CH for ChaosNet
      - HS for Hesiod
  - Special characters
    - ; (comment)
    - @(The current domain name)
    - () (allow data to span lines)
    - * (wild card character, *name* field only)

The DNS Database – Resource Record (2)

- Type of resource record discussed later
  - Zone records: **identify domains and name servers**
    - **SOA**
    - **NS**
  - Basic records: **map names to addresses and route mail**
    - **A**
    - **PTR**
    - **MX**
  - Optional records: **extra information to host or domain**
    - **CNAME**
    - **TXT**
    - **LOC**
    - **SRV**
    - **NSEC, RRSIG, DS, DNSKEY, KEY**

The DNS Database – Resource Record (3)

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone of authority
	NS	Name Server	Identifies zone servers, delegates subdomains
Basic	A	IPv4 Address	Name-to-address translation
	AAAA	Original IPv6 Address	Now obsolete, DO NOT USE
	A6	IPv6 Address	Name-to-IPv6-address translation (V9 only)
	PTR	Pointer	Address-to-name translation
	DNAME	Redirection	Redirection for reverse IPv6 lookups (V9 only)
	MX	Mail Exchanger	Controls email routing
Security	KEY	Public Key	Public key for a DNS name
	NXT	Next	Used with DNSSEC for negative answers
	SIG	Signature	Signed, authenticated zone
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	LOC	Location	Geographic location and extent[a]
	RP	Responsible Person	Specifies per-host contact info
	SRV	Services	Gives locations of well-known services
	TXT	Text	Comments or untyped information

The DNS Database – Resource Record (4)

- SOA: Start Of Authority
  - Defines a DNS zone of authority, each zone has exactly one SOA record.
  - Specify the name of the zone, the technical contact and various timeout information
  - Format:
    - **[zone] IN SOA [server-name] [administrator's mail] (serial, refresh, retry, expire, ttl)**
  - Ex:

;	means comments
@	means current domain name
( )	allow data to span lines
*	Wild card character

```
$TTL 3600;
$ORIGIN cs.nctu.edu.tw.
@     IN     SOA    dns.cs.nctu.edu.tw.   root.cs.nctu.edu.tw.   (
                    2007052102            ; serial number
                    1D                    ; refresh time for slave server
                    30M                   ; retry
                    1W                    ; expire
                    2H     )              ; minimum
```

The DNS Database – Resource Record (5)

- NS: Name Server
  - Identify the authoritative server for a zone
  - Usually follow the SOA record
  - Every authoritative name servers should be listed both in current domain and parent domain zone files
    - Delegation purpose
    - Ex: cs.nctu.edu.tw and nctu.edu.tw

```
$TTL 3600;
$ORIGIN cs.nctu.edu.tw.
@       IN      SOA     dns.cs.nctu.edu.tw.    root.cs.nctu.edu.tw.    (
                        2007052102              ; serial number
                        1D                      ; refresh time for slave server
                        30M                     ; retry
                        1W                      ; expire
                        2H      )               ; minimum
        IN      NS      dns.cs.nctu.edu.tw.
        IN      NS      dns2.cs.nctu.edu.tw.
```

The DNS Database – Resource Record (6)

- A record: Address
  - Provide mapping from hostname to IP address
  - Ex:

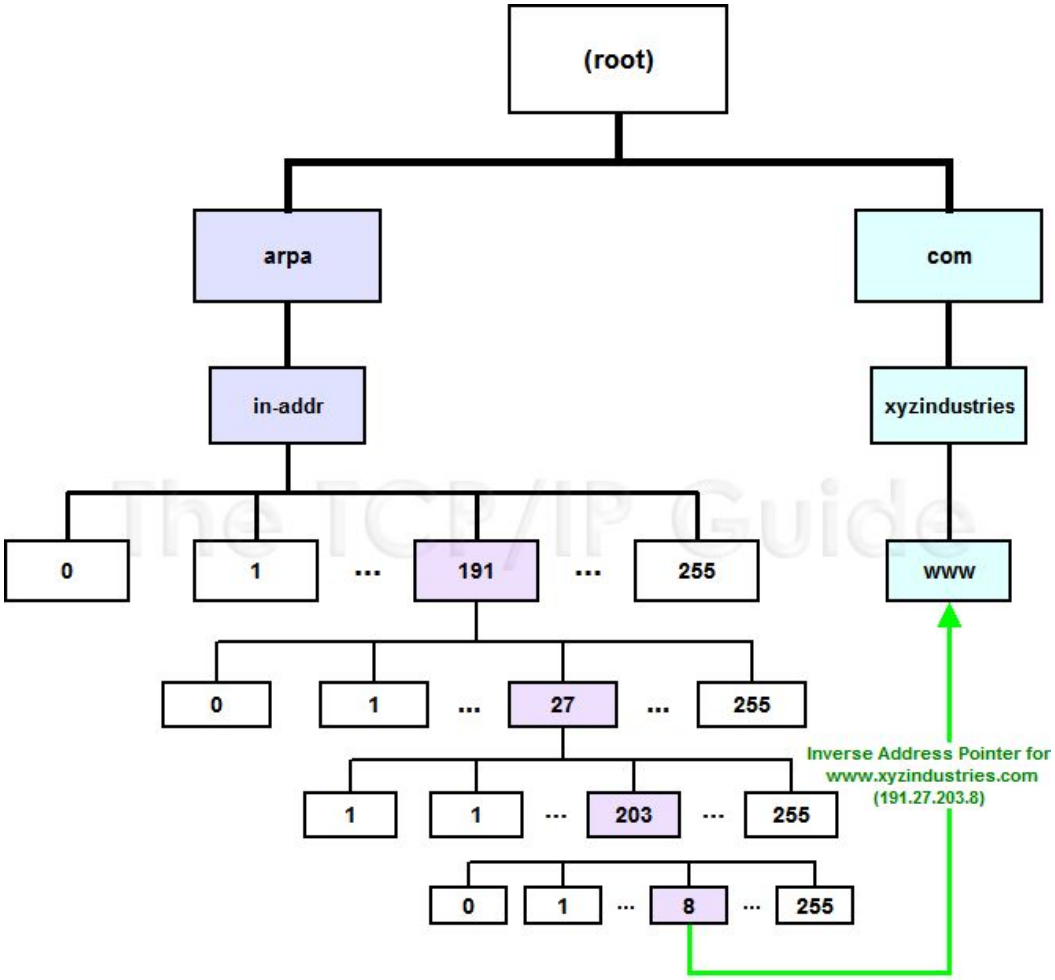
```
$ORIGIN cs.nctu.edu.tw.
@       IN      NS      dns.cs.nctu.edu.tw.
        IN      NS      dns2.cs.nctu.edu.tw.
dns     IN      A       140.113.235.107
dns2    IN      A       140.113.235.103

www     IN      A       140.113.235.111
```

The DNS Database – Resource Record (7)

- PTR: Pointer
  - Perform the reverse mapping from IP address to hostname
  - Special top-level domain: in-addr.arpa
    - ➢ Used to create a naming tree from IP address to hostnames

```
$TTL 259200;
$ORIGIN 235.113.140.in-addr.arpa.
@       IN      SOA     dns.cs.nctu.edu.tw. root.cs.nctu.edu.tw.    (
                        2007052102              ; serial
                        1D                      ; refresh time for secondary server
                        30M                     ; retry
                        1W                      ; expire
                        2H)                     ; minimum
        IN      NS      dns.cs.nctu.edu.tw.
        IN      NS      dns2.cs.nctu.edu.tw.
$ORIGIN in-addr.arpa.
103.235.113.140         IN PTR csmailgate.cs.nctu.edu.tw.
107.235.113.140         IN PTR csns.cs.nctu.edu.tw.
```

The DNS Database – Resource Record (8)



The DNS Database – Resource Record (9)

- MX: Mail exchanger
  - Direct mail to a mail hub rather than the recipient's own workstation
  - Ex:

```
$TTL 3600;
$ORIGIN cs.nctu.edu.tw.
@     IN    SOA    dns.cs.nctu.edu.tw.   root.cs.nctu.edu.tw.   (
                   2007052102     ; serial number
                   1D             ; refresh time for slave server
                   30M             ; retry
                   1W              ; expire
                   2H     )        ; minimum
      IN    NS     dns.cs.nctu.edu.tw.
      IN    NS     dns2.cs.nctu.edu.tw.
      7200  IN   MX  1 csmx1.cs.nctu.edu.tw.
      7200  IN   MX  5 csmx2.cs.nctu.edu.tw.

csmx1  IN    A     140.113.235.104
csmx2  IN    A     140.113.235.105
```

The DNS Database – Resource Record (10)

- CNAME: Canonical name
  - nikename [ttl] IN CNAME hostname
  - Add additional names to a host
    - ➢ To associate a function or to shorten a hostname
  - CNAME record can nest eight deep in BIND
  - Other records must refer to its real hostname
  - Not for load balance
  - Ex:

```
www          IN   A      140.113.209.63
             IN   A      140.113.209.77
penghu-club  IN   CNAME  www
King         IN   CNAME  www

R21601       IN   A      140.113.214.31
superman     IN   CNAME  r21601
```

The DNS Database – Resource Record (11)

- TXT: Text
  - Add arbitrary text to a host's DNS records

```
$TTL 3600;
$ORIGIN cs.nctu.edu.tw.
@       IN      SOA     dns.cs.nctu.edu.tw.    root.cs.nctu.edu.tw.    (
                        2007052102      ; serial number
                        1D              ; refresh time for slave server
                        30M             ; retry
                        1W              ; expire
                        2H      )       ; minimum
        IN      NS      dns.cs.nctu.edu.tw.
        IN      NS      dns2.cs.nctu.edu.tw.

        IN      TXT     "Department of Computer Science"
```

The DNS Database – Resource Record (12)

- LOC: Location
  - Describe the geographic location and physical size of a DNS object
  - Format:
    - name [ttl] IN LOC latitude longitude [altitude [size [hp [vp]]]]
      - latitude 緯度
      - longitude 經度
      - altitude 海拔
      - size: diameter of the bounding sphere
      - hp: horizontal precision
      - vp: vertical precision

```
caida.org.      IN    LOC  32 53 01 N 117 14 25 W 107m 30m 18m 15m
```

The DNS Database – Resource Record (13)

- SRV: Service
  - Specify the location of services within a domain
  - Format:
    - service.proto.name [ttl] IN SRV pri weight port target
  - Ex:

```
; don't allow finger
finger.tcp        SRV  0    0    79    .
; 1/4 of the connections to old, 3/4 to the new
ssh.tcp           SRV  0    1    22    old.cs.colorado.edu.
ssh.tcp           SRV  0    3    22    new.cs.colorado.edu.
; www server
http.tcp          SRV  0    0    80    www.cs.colorado.edu.
                  SRV  10   0    8000  new.cs.colorado.edu
; block all other services
*.tcp        SRV  0    0    0     .
*.udp             SRV  0    0    0     .
```

The DNS Database – Resource Record (14)

- Glue record – Link between zones
  - Parent zone needs to contain the NS records for each delegated zone
  - Ex: In zone files of nctu, it might contain:

```
cs          IN   NS   dns.cs.nctu.edu.tw.
            IN   NS   dns2.cs.nctu.edu.tw.
dns.cs           IN   A    140.113.235.107
dns2.cs          IN   A    140.113.235.103

ee          IN   NS   ns.ee.nctu.edu.tw.
            IN   NS   dns.ee.nctu.edu.tw.
            IN   NS   reds.ee.nctu.edu.tw.
ns.ee            IN   A    140.113.212.150
dns.ee           IN   A    140.113.11.4
reds.ee          IN   A    140.113.202.1
```

- Lame delegation
  - DNS subdomain administration has delegate to you and you never use the domain or parent domain's glue record is not updated