Chapter II
TCP/IP Infrastructure: DNS

Functions of the Domain Name System

- DNS is used to resolve host domain names to IP addresses and find services
- DNS is an essential service for a network that uses Active Directory
- DNS is also required if you want resources such as Web servers available on the Internet
- The most common operating system DNS is implemented on is UNIX/Linux, and this can be integrated with the Windows version of DNS

Host Domain Name Resolution

- Host domain names are used because they are easier to remember than IP addresses
- When a program uses a host domain name, the host domain name must be converted to an IP address before the resource can be contacted

Host or Domain Name Resolution

- The contents of a hosts file are a list of IP addresses and host domain names
- The steps followed by Windows Server 2003 to resolve host domain names are:
  - Host domain name is checked
  - Hosts file is loaded into cache
  - DNS cache is searched
  - DNS server is queried

Host Domain Name Resolution

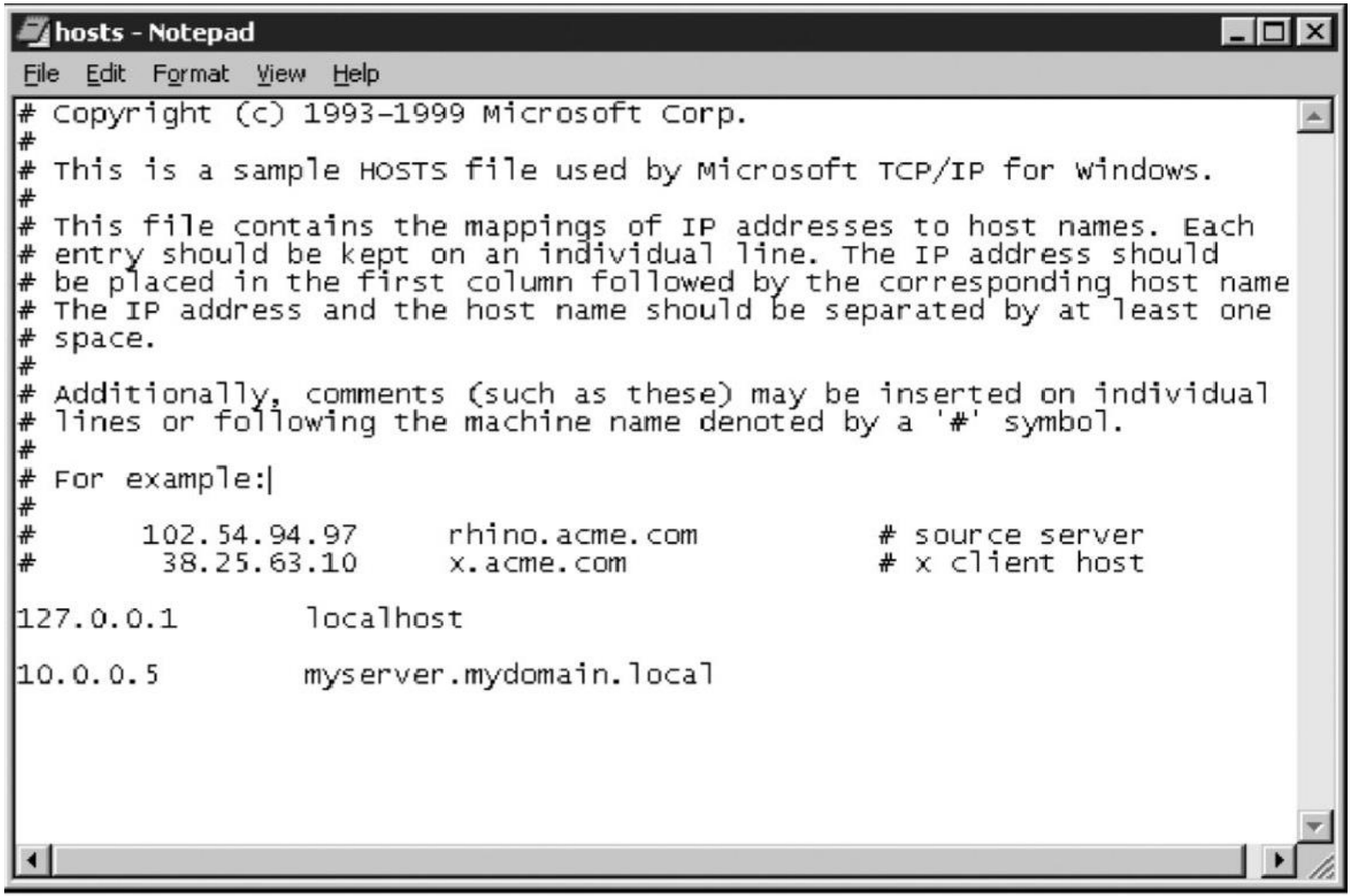
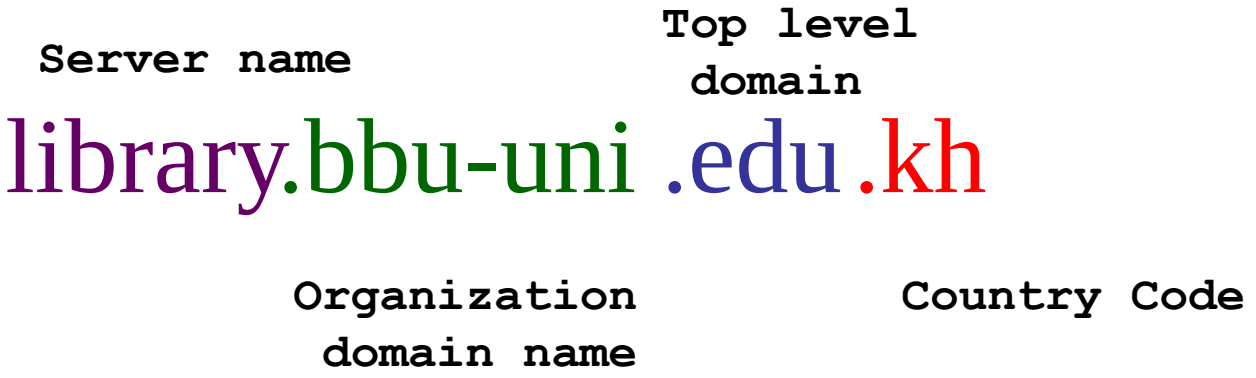


Figure 7-1 Hosts file

DNS Addresses

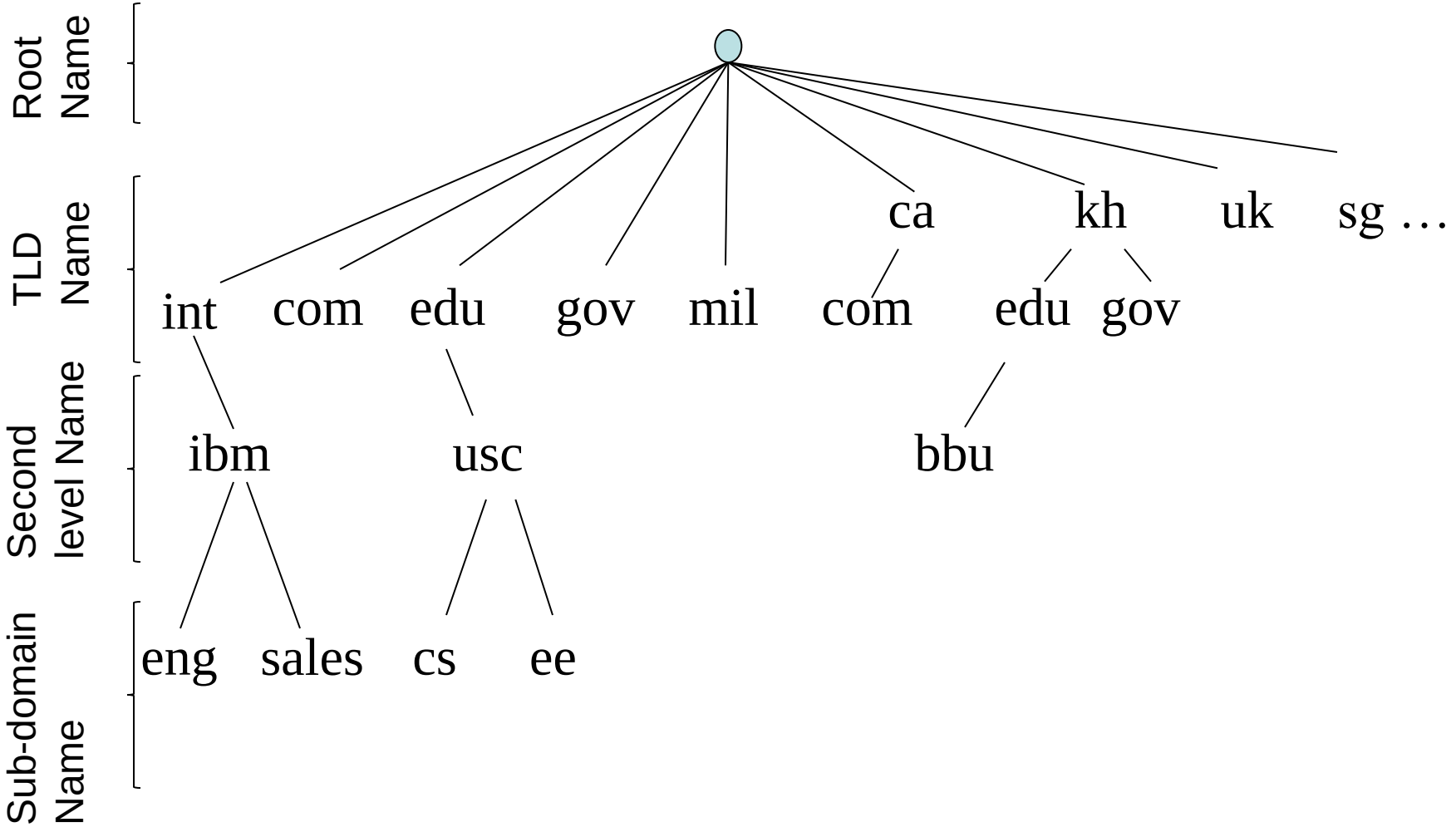
- DNS addresses, also known as Fully Qualified Domain Name **(FQDN)**, are a collection of zone information proceeded by a host name.
- Each element is separated by a period.
- A DNS address is read from back to front or right to left.



- kh, edu, and bbu-uni are all separate zones, hosted on separate DNS servers. Host name library is part of the bbu-uni zone.

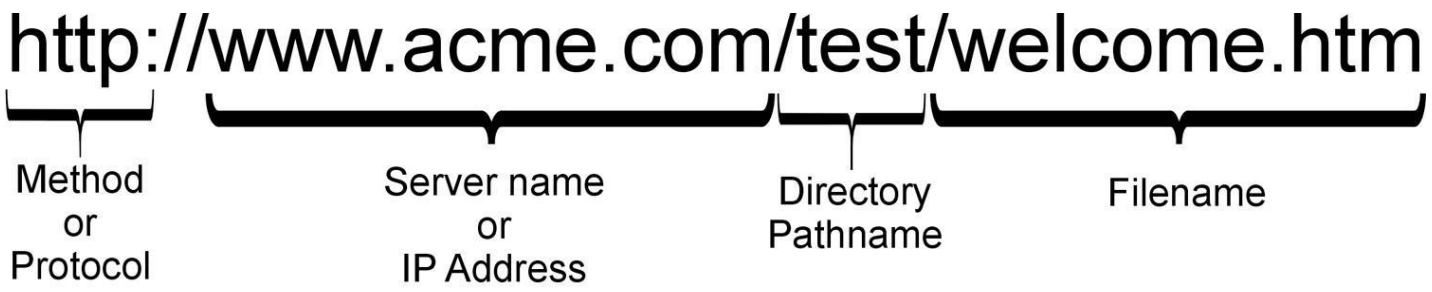
DNS Name Space

- Tree-based hierarchy.

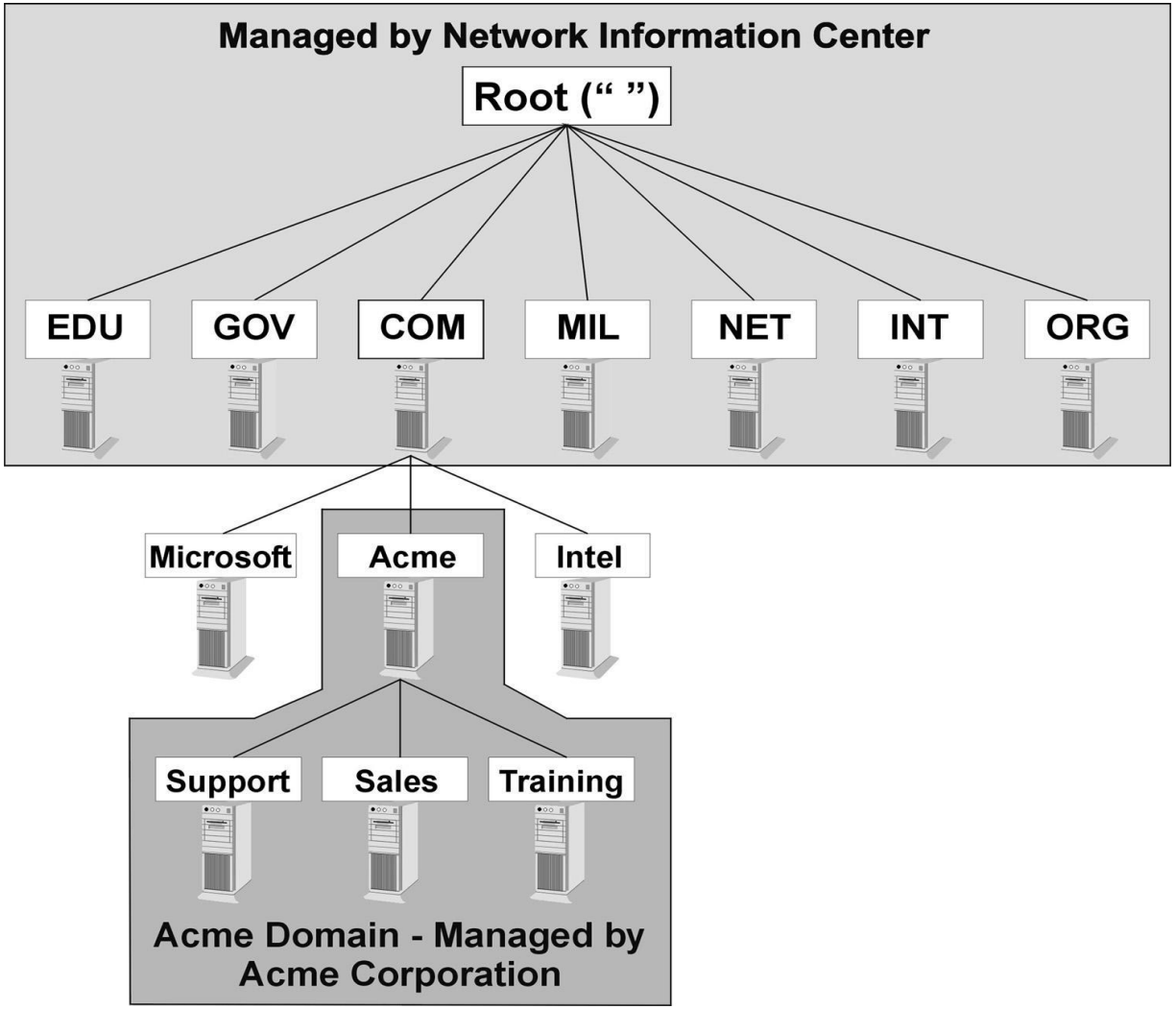


Name Space Structure

- Top-level domains:
  - Generic.
  - Countries.
- Leaf domains: no sub-domains.
- In practice all US organizations are under a generic domain, while everything outside the US is under the corresponding country domain.



Generic DNS Name Space



DNS Names

- Domain names:
  - Concatenation of all domain names starting from its own all the way to the root separated by “.”.
  - Refers to a tree node and all names under it.
  - Case insensitive.
  - Components up to 63 characters.
  - Full name less than 255 characters.

Name Space Management

- Domains are autonomous.
  - Organizational boundaries.
  - Each domain manages its own name space independently of other domains.
- Delegation:
  - When creating new domain: register with parent domain.
    - For name uniqueness.
    - For name resolution.

Hierarchical Structure of DNS

- Root is the top of the tree (root domain) shown as “.” period
- Top level domains – indicate countries and organization type
  - 2 letters for countries (US, UK, FR, CA, **KH**)
  - 3 letters indicate type of org (.com, .**edu**, .org)

Hierarchical Structure of DNS

- Second level domains – variable length names register to individual or organization
  - **Microsoft.**com, **cisco.**com, **bbu.**edu.kh, **sica.**com.uk, **msn.**com.tw (parent domains)
- Sub-domain names – department or geographical location
  - Support, sales, training, south, west (child domains)
- Host domain name (FQDN) – name assigned to a specific computer, this identifies the TCP/IP host, is seen as a leaf of the tree
  - Multiple host names can be associated with the same IP, but only one host name can be given to a computer

Registering a Domain Name

- To participate in the worldwide DNS lookup system, you must register your domain name with a registrar
- A top-level domain (TLD) name is the highest level of domain in the DNS system
- A registrar is an organization that puts domain information into the top-level domain DNS servers so that your domain will be integrated with the worldwide DNS system

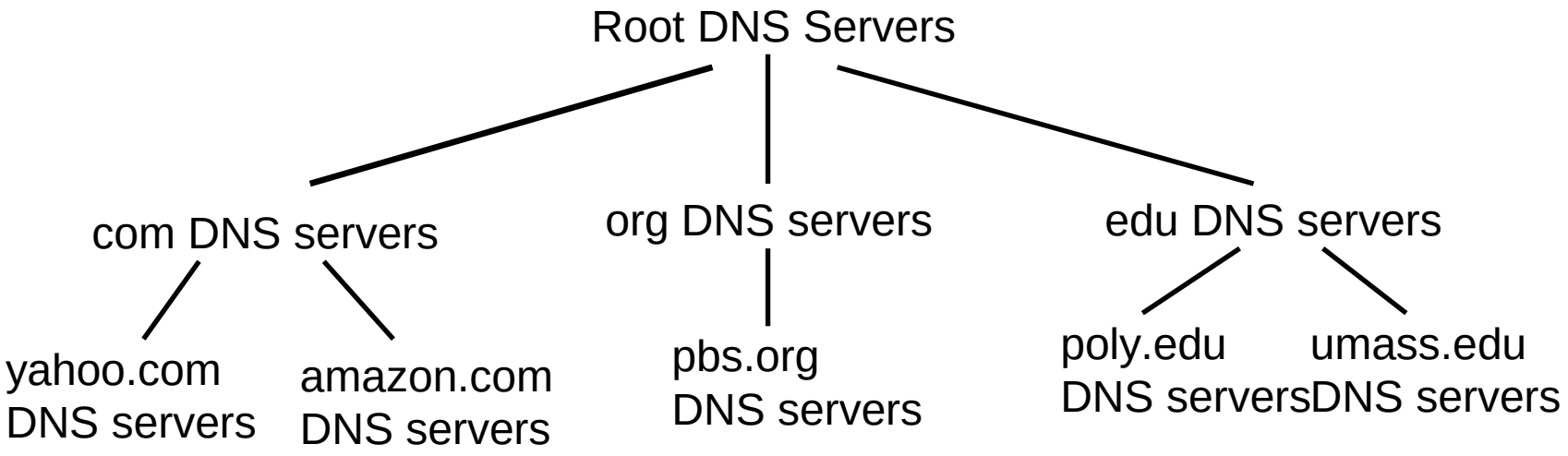
Name Servers

- Name server store DNS databases about name spaces and FQDN
- DNS database is partitioned into **zones**.
- Each zone contains part of the DNS tree.
- Zone <-> name server.
  - Each zone may be served by more than 1 server.
  - A server may serve multiple zones.
- Primary and secondary name servers.

Name Servers

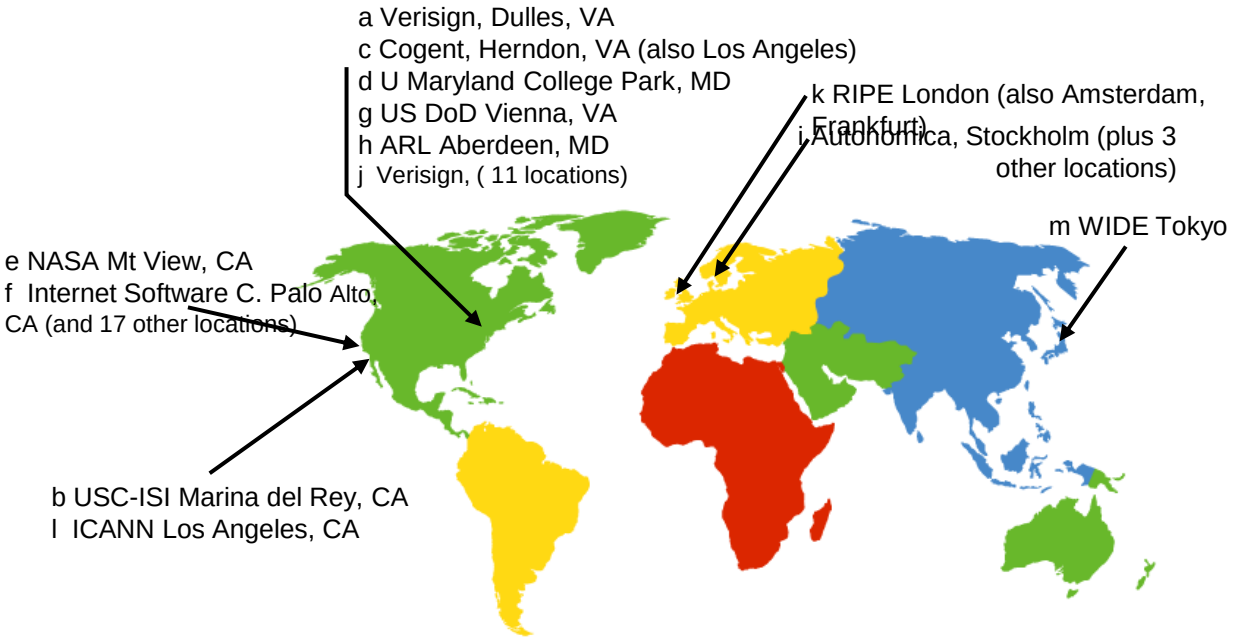
- There are three commonly name servers for hierarchical name space management on the internet:
  - Root Name Servers for register TLD Name
  - Top-Level Domain Name Servers for register Second level Domain Name
  - Local Name Servers for register FQDN and other Resource Records
- All types of Name Servers are involved with the translation of FQDN to IP (DNS name Resolution)

Distributed, Hierarchical Database



DNS: Root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server



13 root name servers worldwide

TLD and Authoritative Servers

- Top-level domain (TLD) servers: responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.
  - Network solutions maintains servers for com TLD
  - Educause for edu TLD
- Authoritative DNS servers: organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web and mail).
  - Can be maintained by organization or service provider

Local Name Server

- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one.
  - Also called “default name server”
- When a host makes a DNS query, query is sent to its local DNS server
  - Acts as a proxy, forwards query into hierarchy.

Local Name or DNS Servers

- Almost all LANs have a local DNS server.
- Clients on the LAN address all DNS requests to the local DNS server.
- The local DNS server either returns the answer to the request from its own database, or it will query other DNS servers to locate the answer.
- Today, many DNS servers can be **automatically updated**, so that hosts that have different IP addresses can be easily contacted via DNS name.

DNS: caching and updating records

- once (any) name server learns mapping, it *caches* mapping
  - cache entries timeout (disappear) after some time
  - TLD servers typically cached in local name servers
    - Thus root name servers not often visited
- update/notify mechanisms under design by IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

Name Resolution (1)

- Application wants to resolve name.
- Resolver sends recursive query to local name server.
  - If Resolver is configured with list of local name servers, it select servers in round-robin fashion.
- If name is local, local name server returns matching *authoritative* RRs.
  - *Authoritative* RR comes from authority managing the RR and is always correct.
  - *Cached* RRs may be out of date.

Name Resolution (2)

- If information not available locally (not even cached), local NS will have to ask someone else using iterative queries.
- Iterative resolution
  - Name server not able to resolve query, sends back the name of the next server to try.
  - Some servers use this method.
  - More control for clients.

DNS Lookup Process for Name Resolution

- If FQDN name is requested to a DNS service, it will return its IP.
  - DNS clients are resolvers
  - DNS Servers are name servers
  - Host files were first used, but became unmanageable
  - Recursive query – must have good answer or error
  - Iterative query – gives a best answer, it's here or here is the best chance place to look
- A DNS Client Will Use a Recursive Query With the Preferred Server to Find an IP Address. While the Preferred Server Will Typically Use an Iterative Query to Discover the IP Address

DNS Lookup Process

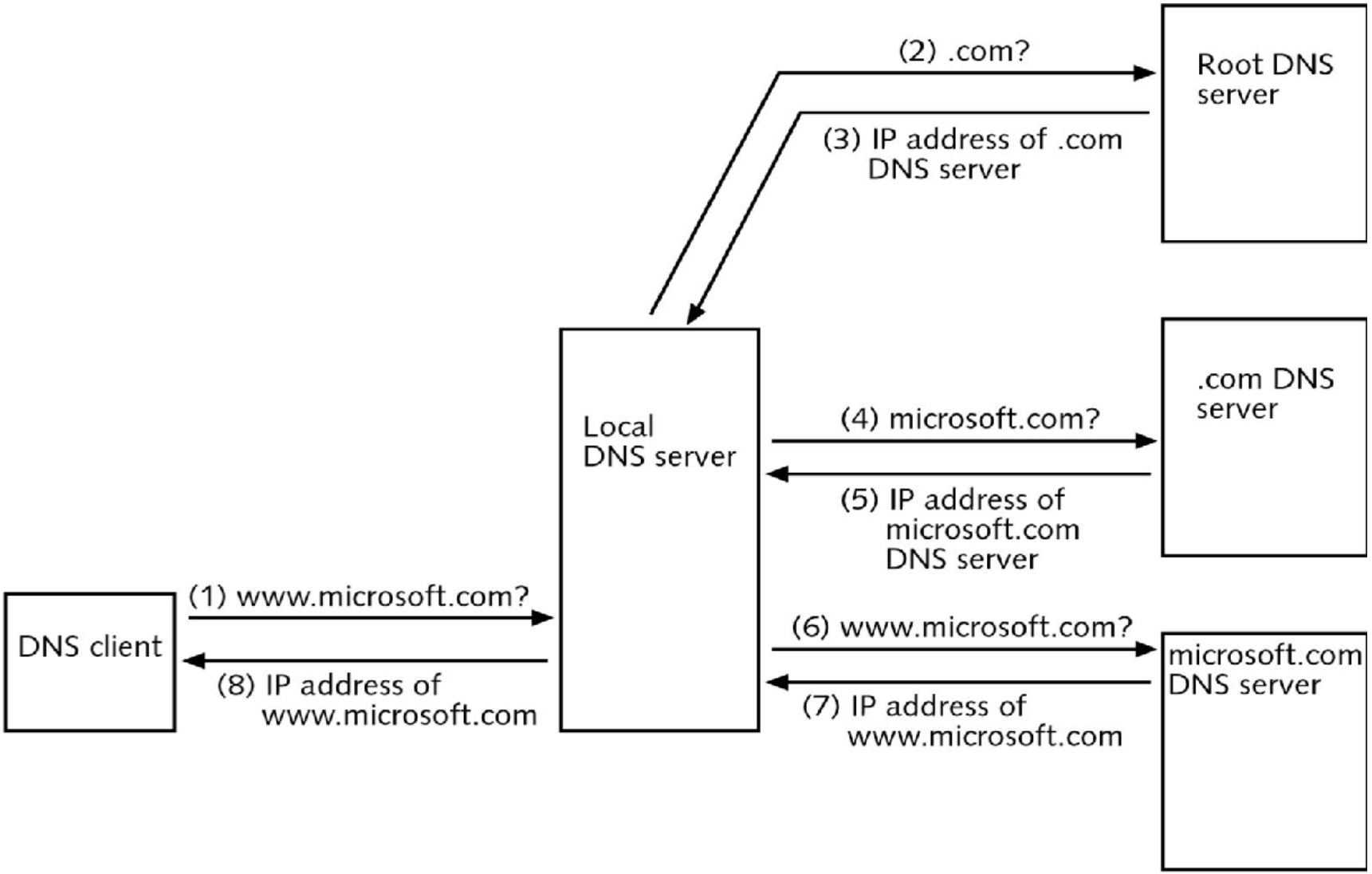
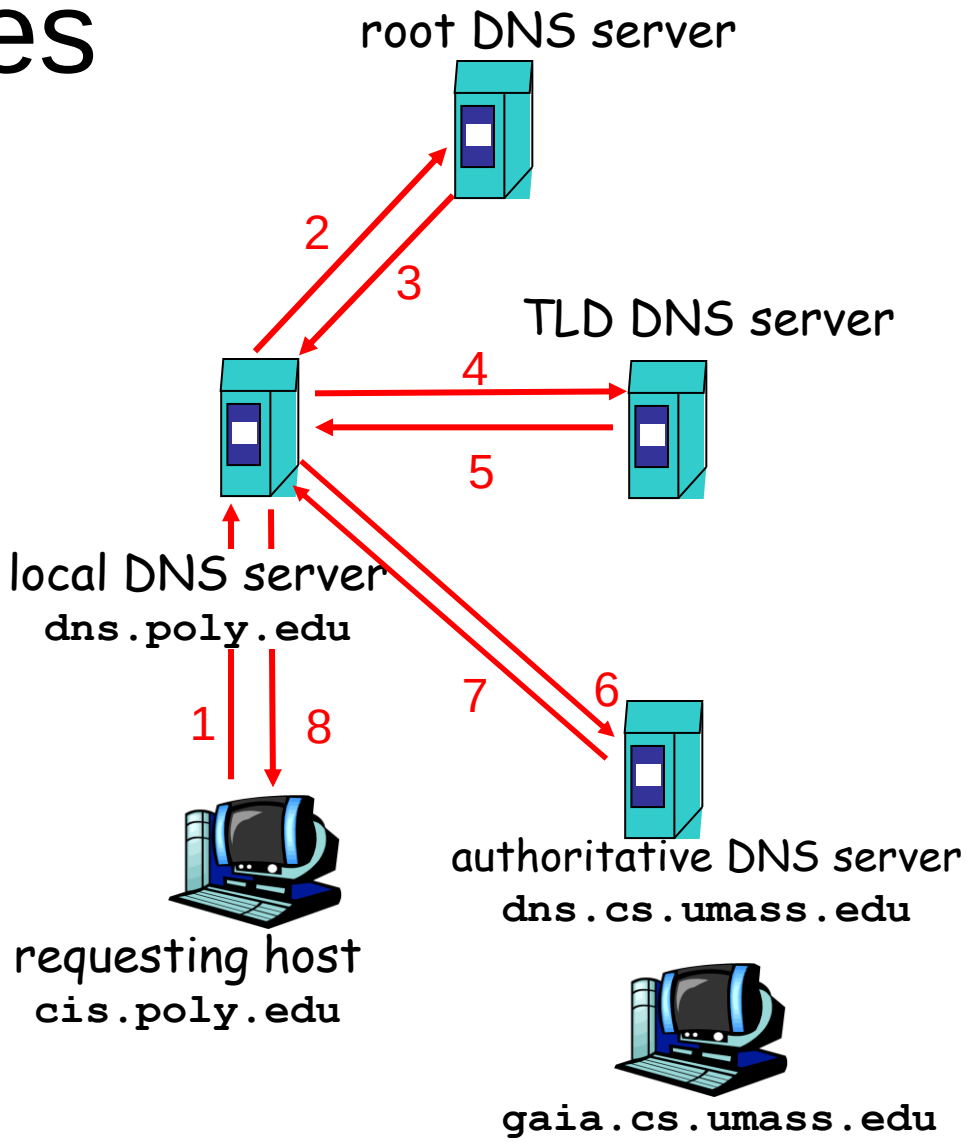


Figure 7-2 DNS lookup process

Iterative Queries

iterated query:

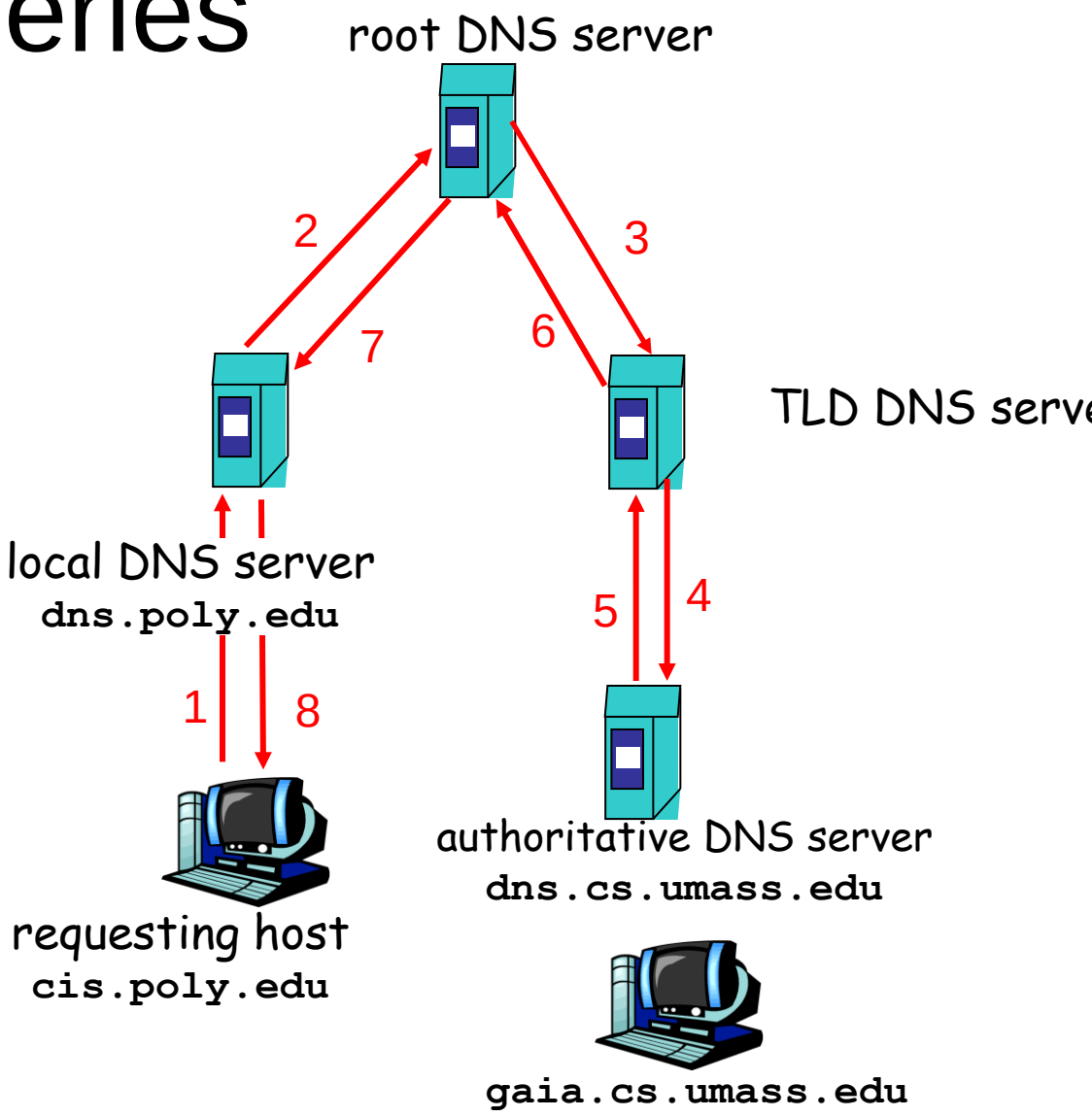
- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



Recursive queries

recursive query:

- puts burden of name resolution on contacted name server
- heavy load?



Forward Lookup

- When a DNS server resolves a host name to an IP address it is known as forward lookup
- Resolving host names within an organization is a two-packet process
- In recursive lookup a DNS query that is resolved through other DNS servers until the requested information is located

Reverse Lookup

- When DNS is used to resolve IP addresses to host names, the process is known as reverse lookup

- A reverse lookup allows you to specify an IP address and the DNS server returns the host name that is defined for it

DNS Record Types

- DNS records are created on a DNS server to resolve queries
- Each type of record holds different information about a service, host name, IP address, or domain
- Different queries request information contained in specific DNS record types

DNS Record Types

- SOA: start of authority.
  - Marks beginning of zone's database.
  - Provides general info about the zone: e-mail address of admin, default TTL, etc.
- A: address.
  - Contains 32-bit IP address.
  - Single name <-> several A RRs.
- MX: mail exchange.
  - Name of mail server for this domain.

DNS Record Types

- NS: name server.
  - Name of name server for this domain.
- CNAME: canonical name.
  - Alias.
- HINFO: host description.
  - Provides information about host, e.g., CPU type, OS, etc.
- TXT: arbitrary string of characters.
  - Generic description of the domain, where it is located, etc.

Installing DNS

- Windows Server 2003 can act as a DNS server
- Can install DNS on multiple servers and you must add DNS individually to each of these servers
- To reduce WAN traffic in large organizations, DNS servers can be placed in each physical location
- To decide the best placement of DNS servers during the planning process, estimate the amount of traffic that will be generated by DNS

DNS Zones

- A DNS zone is the part of the DNS namespace for which a DNS server is responsible
- Once inside the zone, you can create DNS records and subdomains
- When a zone is created, you designate whether it will hold records for forward lookups or reverse lookups
  - Forward lookup zone: holds records for forward lookups (Name to IP)
  - Reverse lookup zone: holds records for reverse lookups (IP to Name)

Primary and Secondary Zones

- Primary and secondary zones are used to synchronize DNS information automatically between DNS servers
- A primary zone is the first to be created, and all of the DNS records are created in the primary zone
- A secondary zone takes copies of primary zone information
- You cannot directly edit the records in a secondary zone because they are copied from the primary zone
- The process of moving information from the primary zone to the secondary zone is called a zone transfer

Stub Zones

- A stub zone is a DNS zone that holds only NS records for a domain
- NS records define the name servers that are responsible for a domain

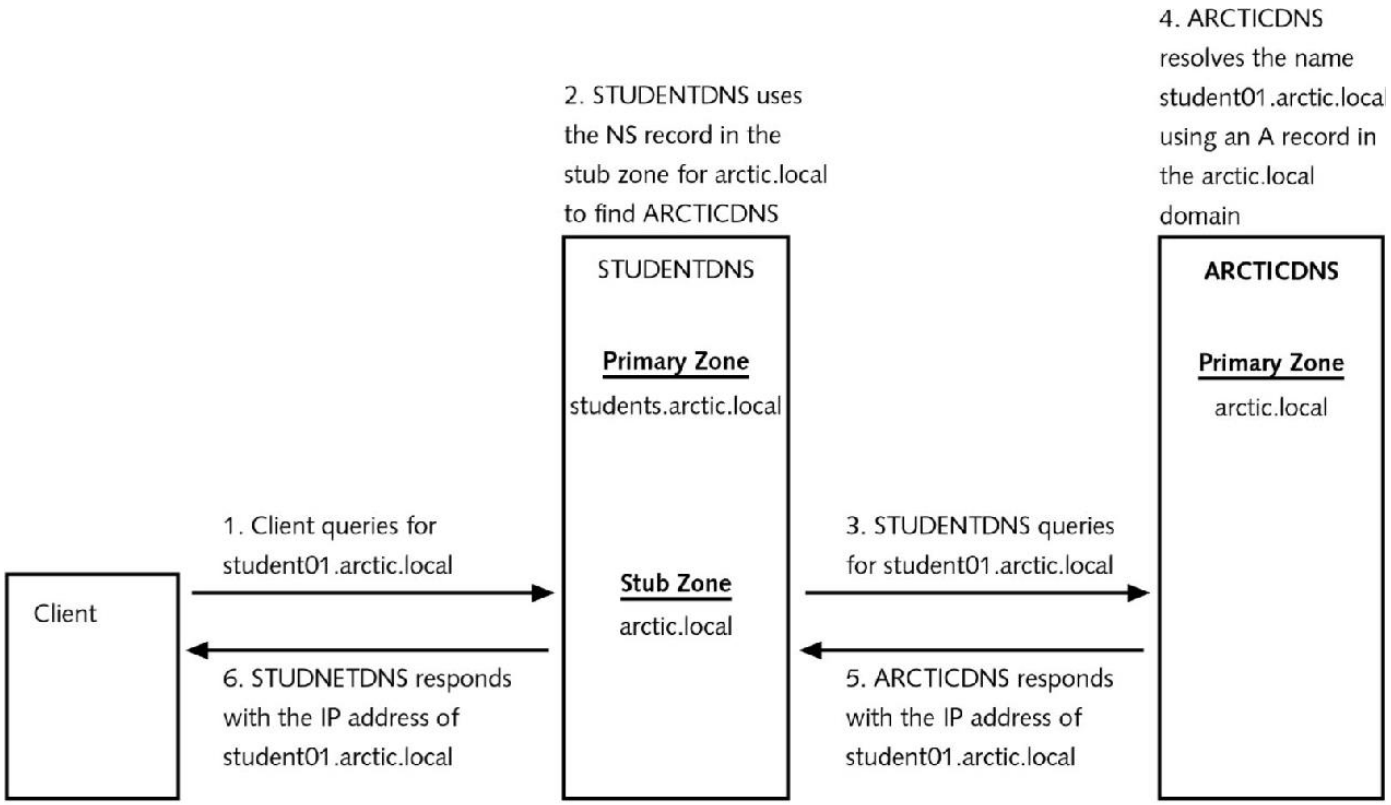


Figure 7-5 DNS lookup using a stub zone

Active Directory and DNS

- Active Directory requires DNS to function properly
- The most important function that DNS performs for Active Directory is locating services, such as domain controllers
- An Active Directory integrated zone stores information in Active Directory rather than in a file on the local hard drive
  - To store DNS information in an Active Directory integrated zone, the DNS server must also be a domain controller

Active Directory Integrated Zones

- Storing DNS information in Active Directory offers the following advantages over traditional primary and secondary zones:
  - Automatic backup of zone information
  - Multimaster replication
  - Increased security

Dynamic DNS and DHCP

- The Dynamic DNS information updated by Windows 2000/XP is negotiated with the DHCP server during the lease process
- By default, a DHCP server running on Windows Server 2003 updates DNS records only for Windows 2000/XP clients and only if requested to do so

WINS Integration

- To integrate with WINS, a DNS zone can be configured with a WINS server to help resolve names
- If a DNS zone receives a query for a host name for which it has no A record, it forwards the request to a WINS server
  - This results in slower response times and increased processor utilization

WINS Integration (continued)

- If DNS and WINS are running on separate servers, it also results in increased network traffic and even slower response times
- Integrating a WINS server with a DNS forward lookup zone creates a WINS record in the zone
- You can specify that records resolved via WINS are not replicated to other DNS servers by selecting the Do not replicate this record check box