Hunan University of Arts and Science

Networking Theory
&
Applications

CIS 291

2018 – 2019

Windows Server® 2012

Part 3A

Windows Server
2012 R2

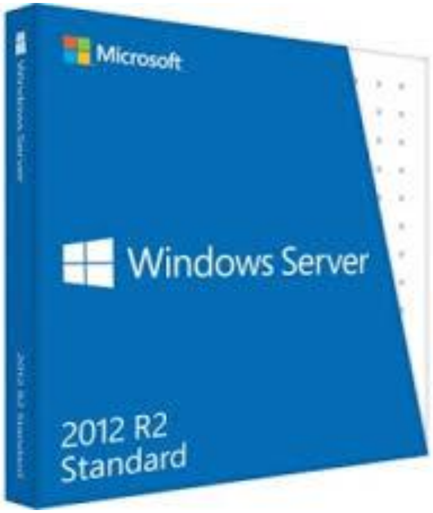
Chapter 4
Deploying and configuring core network services
部署和配置核心网络服务

Objectives in this chapter: 本章的目标

1- Configure IPv4 and IPv6 addressing

2- Configure servers

3- Deploy and configure DNS service



Objective 4.3: Deploy and configure the DNS service

1- Understanding the DNS Architecture

- Host names are easier for us to remember than IP addresses.
- Computers need to resolve the host names we use to IP addresses in order to communicate with other computers.
- This conversion process is referred to as **name resolution**.
- **Host tables** were used In the early days of TCP/IP networking when networks were small, but are impractical today.
- Today, there are millions of computers on the Internet, and the idea of maintaining and distributing a single file containing names for all of them is absurd.
- Since that time we use DNS , **Domain Name System (DNS)** servers convert host names into IP addresses.

Creating a DNS Standard

At its core, the DNS is still a list of names and their equivalent IP addresses, but the methods for creating, storing, and retrieving those names is very different from those in a host table. The DNS consists of three elements:

A. The DNS name space

B. Name servers.

C. Resolvers

A- The DNS Name Space

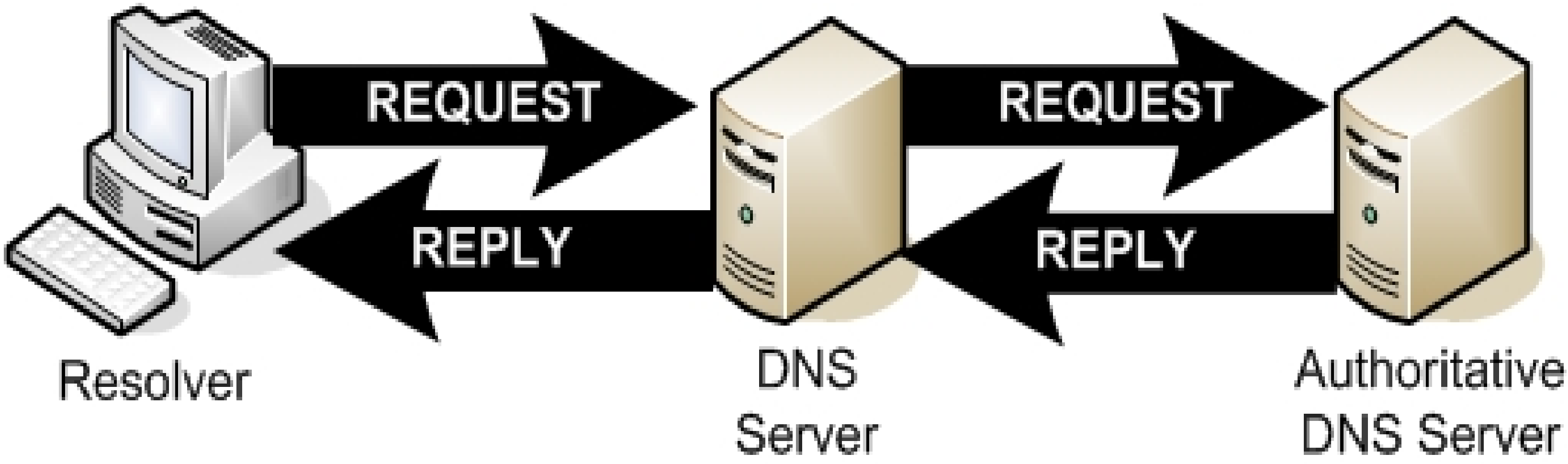
- The DNS standards define a tree-structured name space in which each branch of the tree identifies a **domain**.
- Each domain contains a collection of **resource records** that contain host names, IP addresses, and other information.
- Query operations are attempts to retrieve specific resource records from a particular domain.

B- Name Servers

- A DNS server is an application running on a server computer that maintains information about the domain tree structure and (usually) contains authoritative information about one or more specific domains in that structure.
- The application responds to queries for information about the domains for which it is the authority and forwards queries about other domains to other name servers.
- This enables any DNS server to access information about any domain in the tree.

C- Resolvers

- A **resolver** is a client program that generates DNS queries and sends them to a DNS server for fulfillment.
- A resolver has direct access to at least one DNS server and can also process referrals to direct its queries to other servers when necessary.



DNS servers relay requests and replies to other DNS servers

The DNS name resolution process:

1- A resolver submitting a name resolution request to its designated DNS server.

2- When the server does not possess information about the requested name, it forwards the request to another DNS server on the network.

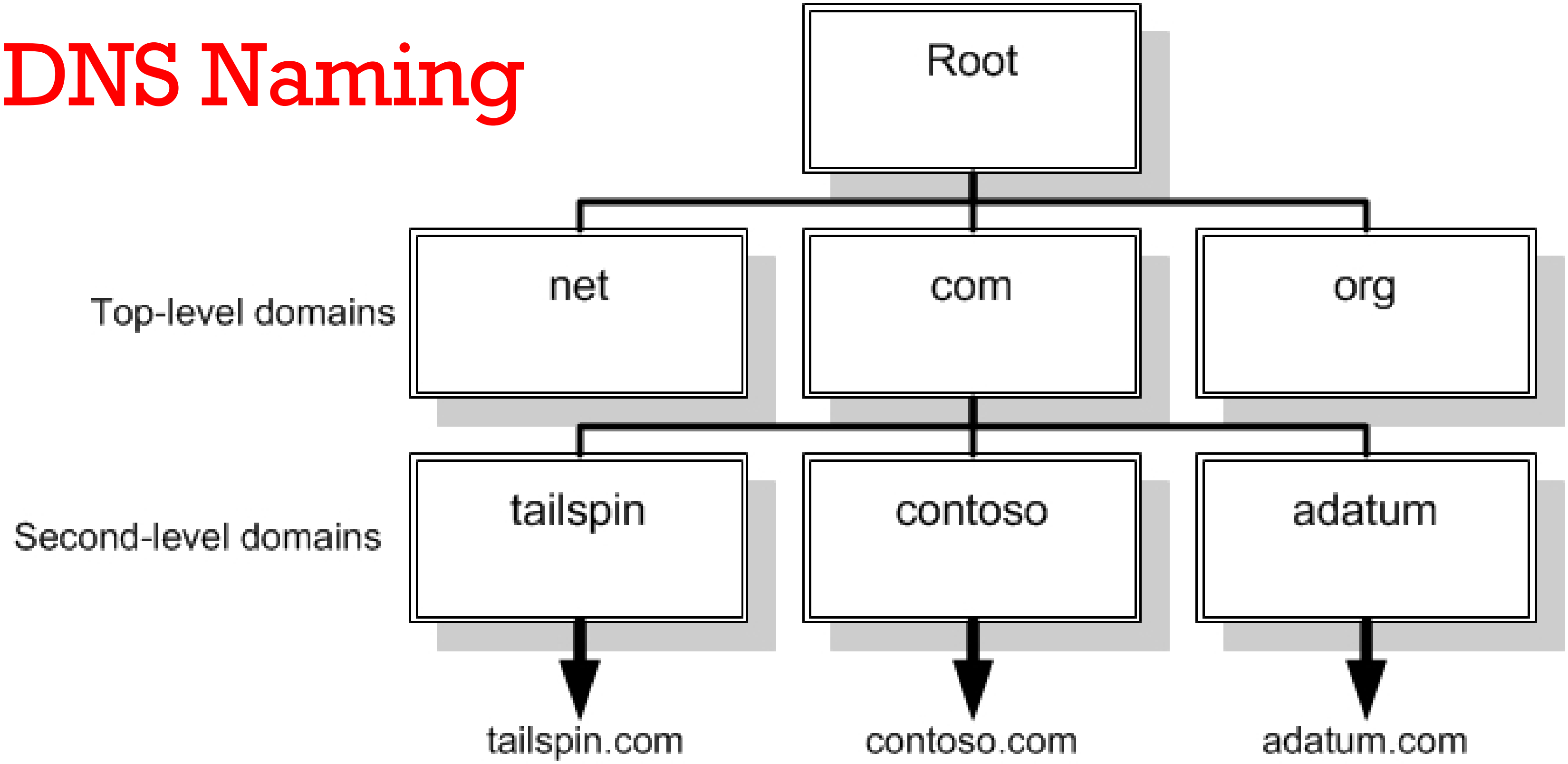
3- The second server generates a response containing the IP address of the requested name and returns it to the first server

4- first server relays the information to the resolver.

2- DNS Naming

- A two-tiered system, consisting of domain names and host names
- Obtain Doman names from a centralized authority, to ensure uniqueness
- Assign the host names within that domain
- Internet websites use this naming method
- We access web servers using a Uniform Resource Locater (URL), such as: http://www.contoso.com

DNS Naming



The DNS domain hierarchy

3- The DNS Domain Hierarchy

- The authoritative source for a domain is the DNS server responsible for maintaining that domain's resource records.
- DNS servers can locate the authoritative source for any domain name, by communicating with other DNS servers.
- Domains at each level of the hierarchy are responsible for maintaining information about the domains in the next lower level.
- The root name servers are the highest-level DNS servers in the entire namespace.
- All DNS server implementations are preconfigured with the IP addresses of the root name servers.

Top-Level Domains

The original DNS name space called for six (general)**generic top-level domains (gTLDs)**, dedicated to specific purposes:

- **com**: Commercial organizations
- **edu**: Four-year, degree-granting educational institutions in North America
- **gov**: United States government institutions
- **mil**: United States military applications
- **net**: Networking organizations
- **org**: Noncommercial organizations

ICANN's New Top-Level Domains

- ICANN is also responsible for the ratification of new top-level domains:
  - aero
  - biz
  - coop
  - info
  - museum
  - name
  - pro
  - asia
  - cat
  - jobs
  - mobi
  - tel
  - travel

Top-Level Domains

- The root name servers do nothing but respond to millions of requests by sending out the addresses of the authoritative servers for the top-level domains.
- The top-level domain servers do the same for the second-level domains.
- There are no hosts in the root or top-level domains.

Country Code Domains

- There are hundreds of two-letter country-code top-level domains (ccTLDs):
  - ✓ fr for France
  - ✓ de for Deutschland (Germany)
  - ✓ us for the United States
  - ✓ ca for Canada
- Each domain is permitted to establish its own prices and requirements for registration of subdomains.

Second-Level Domains

- Each top-level domain has its own collection of second-level domains.
- Individuals and organizations can purchase these domains for their own use.
- To use the domain name, you must supply the registrar with the IP addresses of two DNS servers that you want to be the authoritative sources for information about the domain.
- The administrators of the top-level domain servers then create resource records pointing to these authoritative servers.

Break

4- DNS Messaging

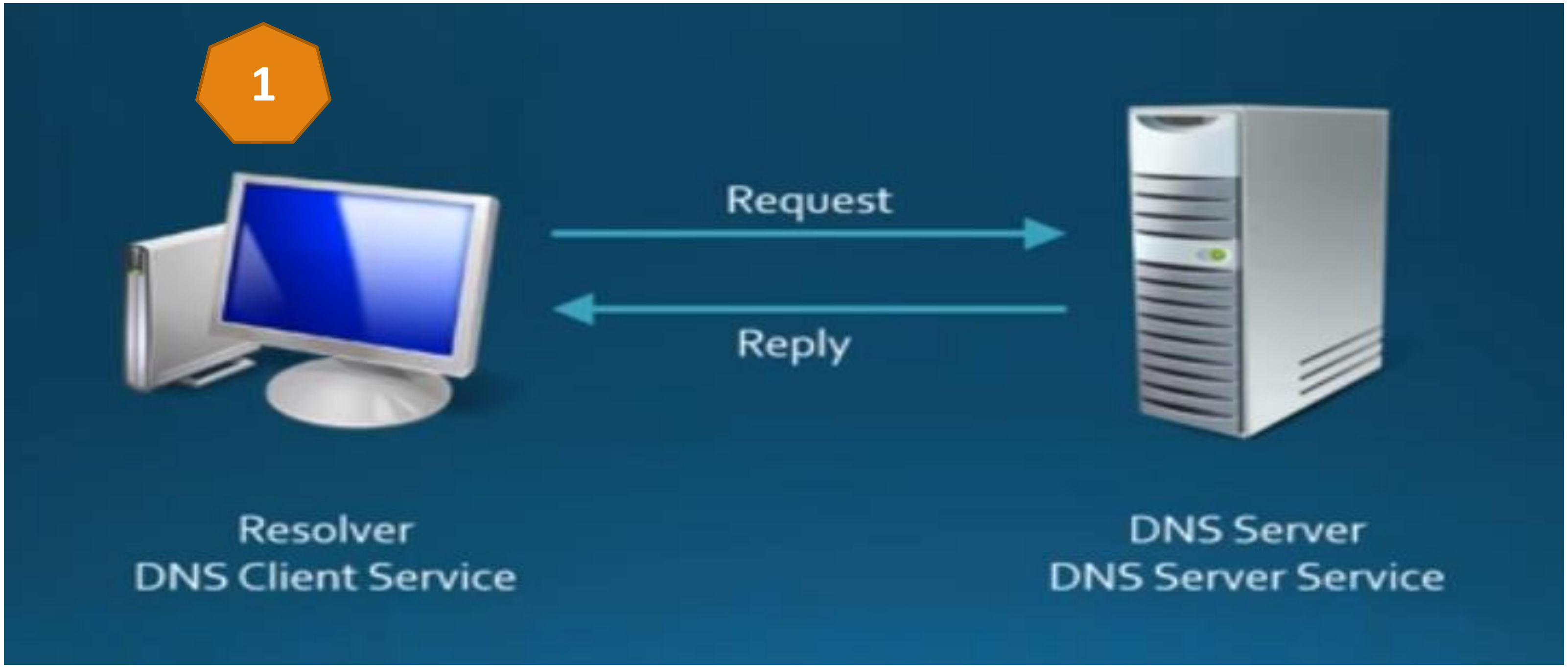
The Domain Name System uses a single message format for all communications that consists of the following five sections:

- **Header:** Contains information about the nature of the message.
- **Question:** Contains the information being requested from the destination server.
- **Answer:** Contains resource records supplying the information requested in the Question section.
- **Authority:** Contains resource records pointing to an authority for the information requested in the Question section.
- **Additional:** Contains resource records with additional information in response to the Question section.

5- DNS Communications

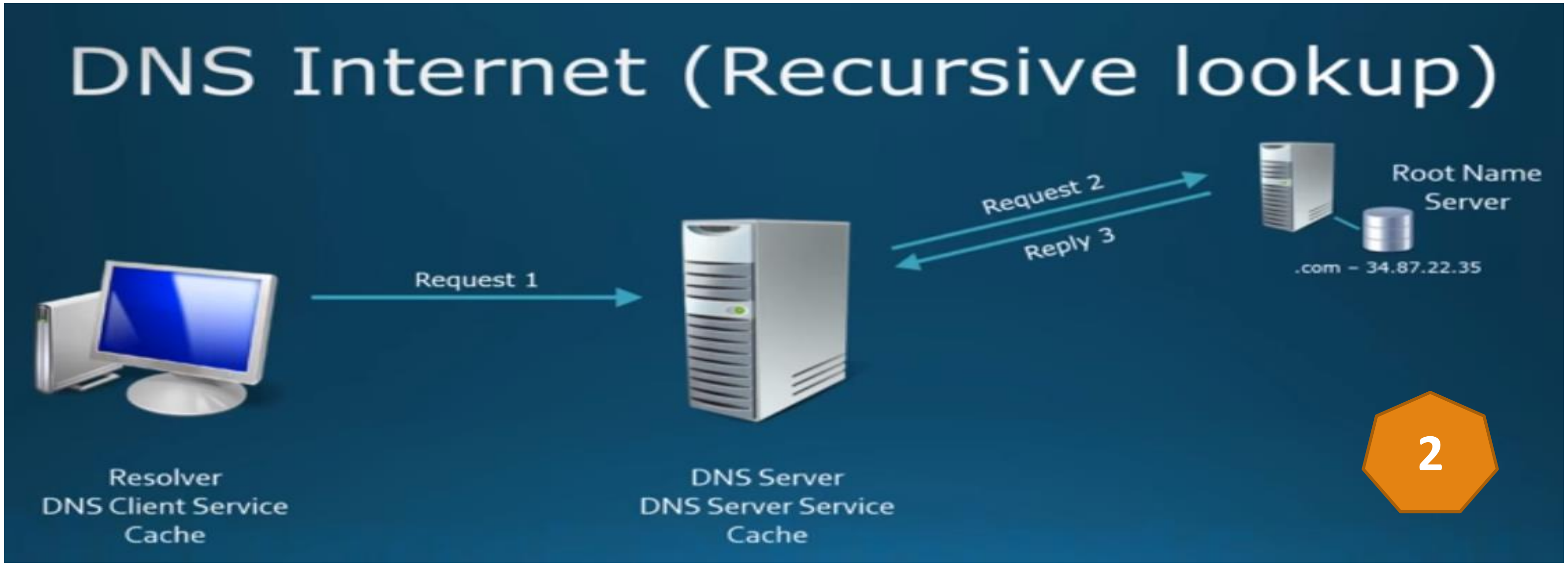
- Type a URL containing a DNS name (**www.microsoft.com**) into the browser's Address box and press Enter.
- You will see a message that says something like "**Finding Site: www.microsoft.com**."
- Then, a few seconds later, you will see a message that says "**Connecting to**," followed by an IP address.
- It is during this interval that the DNS name resolution process occurs.
- To better explain the relationships among the DNS servers for various domains in the namespace, the following procedure diagrams the Internet name resolution process.

1. A user on a client system specifies the DNS name of an Internet server in an application such as a web browser.
2. The application generates an application programming interface (API) call to the resolver on the client system and the resolver creates a DNS recursive query message containing the server name, which it transmits to the DNS server identified in computer's TCP/IP configuration,



A DNS client sends a name resolution request to its designated DNS server

3. The client’s DNS server, after receiving the query, checks its resource records (in its cach)to see if it is the authoritative source for the zone containing the requested server name. If it is not, which is typical, the DNS server generates an iterative query and submits it to one of the root name servers

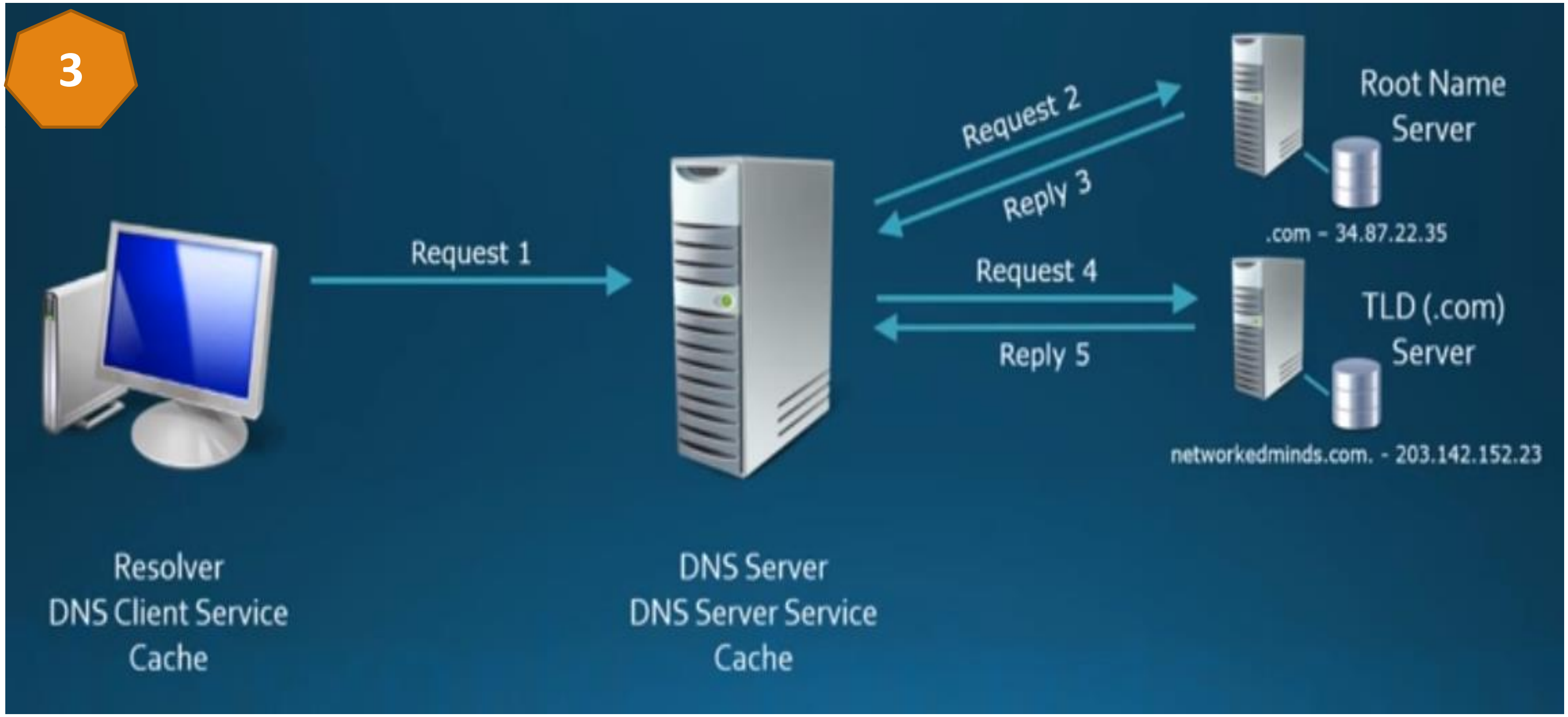


The client’s DNS server forwards an iterative query to a root name server

4. The root name server examines the name requested by the client’s DNS server and consults its resource records to identify the authoritative servers for the name’s top-level domain.

5. The root name server then transmits a reply to the client’s DNS server that contains a referral to the top-level domain server IP addresses.

6. The client's DNS server, now in possession of the top-level domain server address for the requested name, generates a new iterative query and transmits it to the top-level domain server, as shown in Figure 4-17

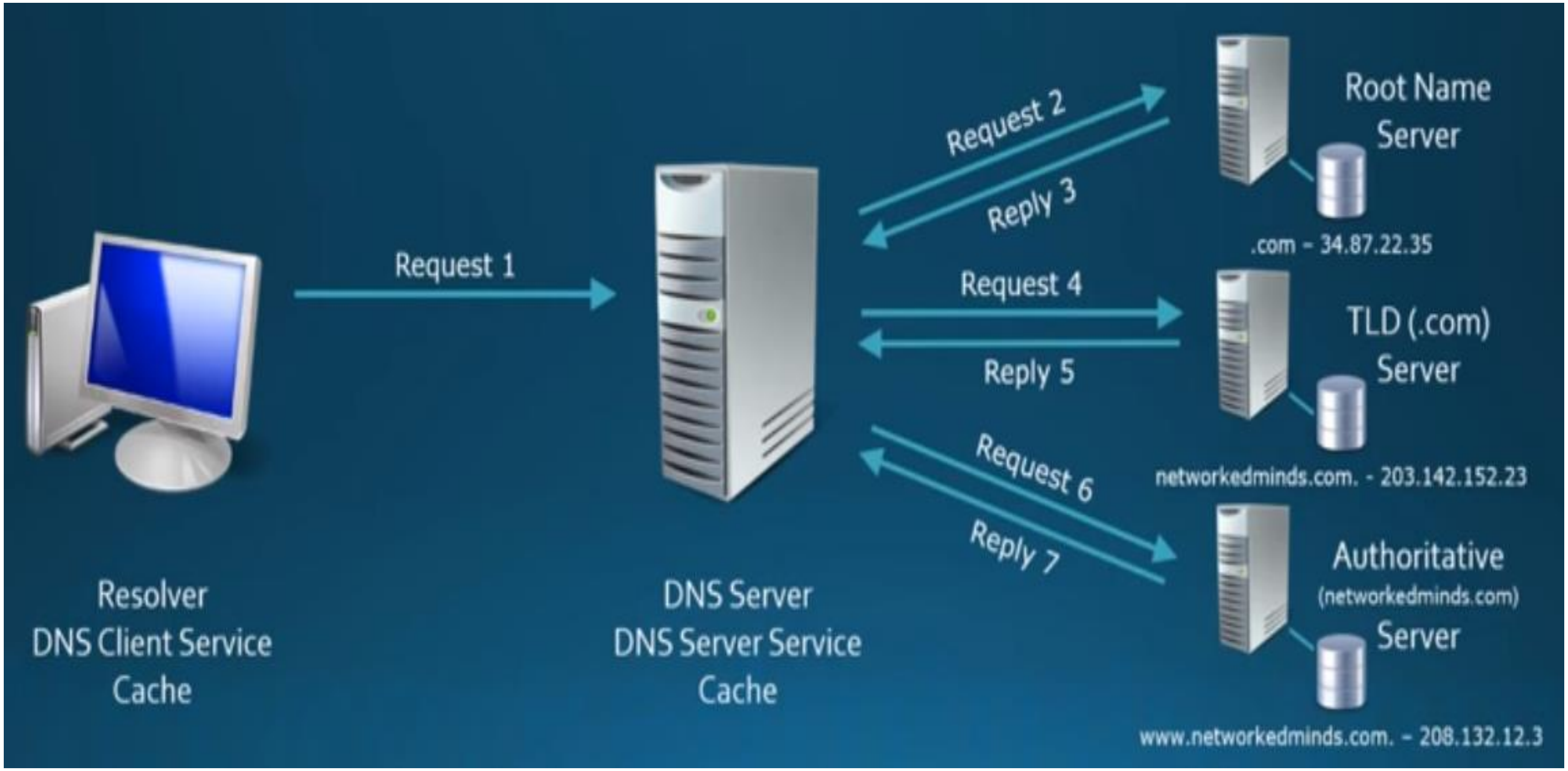


The client's DNS server forwards an iterative query to a top-level domain server

7. The top-level domain server examines the second-level domain in the requested name and transmits a referral containing the addresses of authoritative servers for that second-level domain back to the client's DNS server.

8. The client’s DNS server generates another iterative query and transmits it to the second-level domain server, as shown in Figure 4-18.

9. If the second-level domain server is the authority for the zone containing the requested name, it consults its resource records to determine the IP address of the requested system and transmits it in a reply message back to that client’s DNS server.



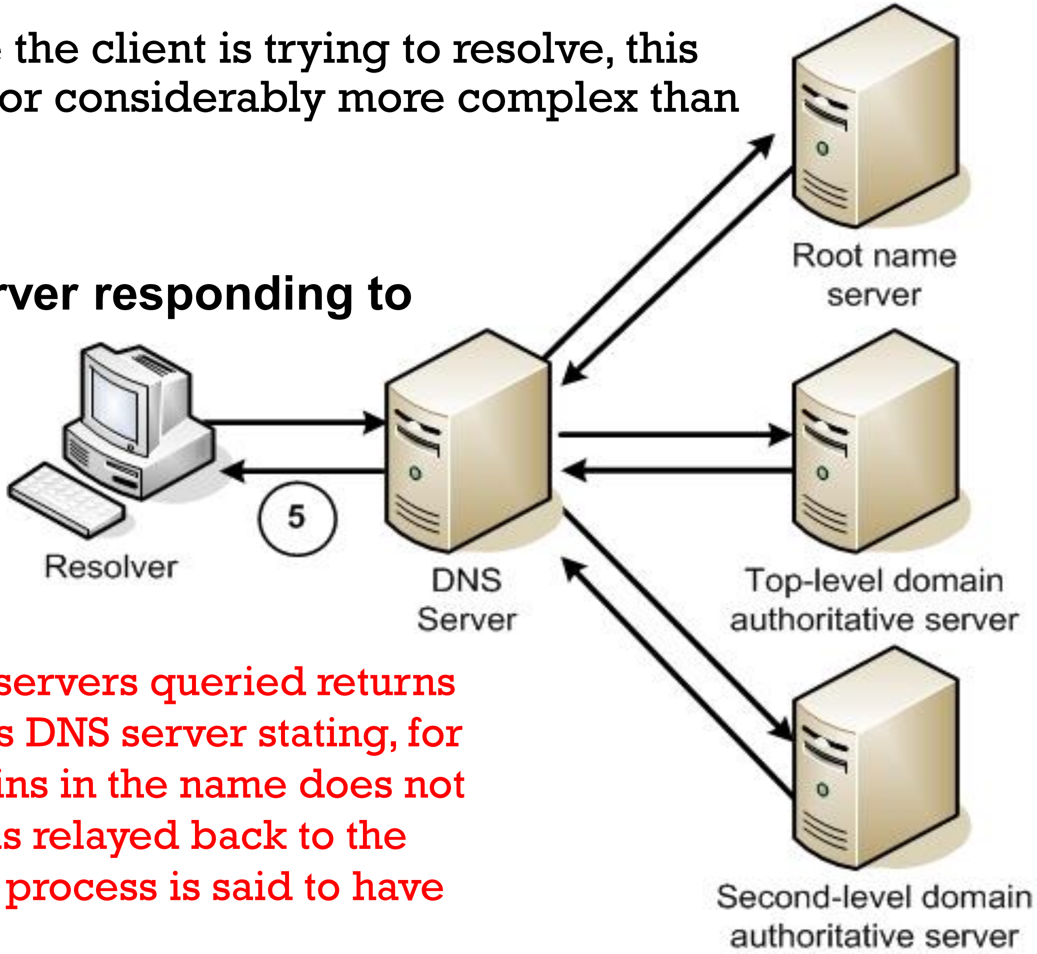
The client’s DNS server forwarding the request to a second-level domain server

10. The client’s DNS server receives the reply from the authoritative server and transmits the IP address back to the resolver on the client system, as shown in Figure 4-19.

11. The resolver relays the address to the application, which can then initiate IP communications with the system specified by the user.

Depending on the name the client is trying to resolve, this process can be simpler or considerably more complex than the one shown here

The client’s DNS server responding to the client resolver


Root name server
Resolver
5
DNS Server
Top-level domain authoritative server
Second-level domain authoritative server

If any of the authoritative DNS servers queried returns an error message to the client’s DNS server stating, for example, that one of the domains in the name does not exist, then this error message is relayed back to the client and the name resolution process is said to have failed