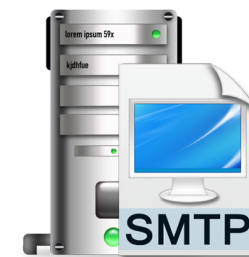


Simple Mail Transfer Protocol

- ❑ Uses **TCP** to reliably transfer email messages from client to server, on port **25**

- ❑ Three phases of transfer
 - ☞ Handshaking (greeting)
 - ☞ Transfer of messages
 - ☞ Closure

- ❑ Command/response interaction
 - ☞ **Commands**: 7-bit ASCII text
 - ☞ **Response**: status code and phrase



Sample SMTP Interaction

S: 220 mx.lentil.edu
C: HELO mx.halva.fr
S: 250 Hello halva.fr, pleased to meet you
C: MAIL FROM: <alice@halva.fr>
S: 250 alice@halva.fr... Sender ok
C: RCPT TO: <bob@lentil.edu>
S: 250 bob@lentil.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like dahl?
C: How about with naan?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 lentil.edu closing connection



Quick exercise

❑ SMTP is a _____ protocol.

☞ A. pull

☞ B. push

☞ C. both a and b

☞ D. none of the above

Tracking of Sent Mail

- ❑ **Original SMTP mail service provides limited mechanisms for tracking a transmitted message, and none for verifying that it has been delivered or read.**

- ❑ **Recommended solution from IETF**
 - ☞ **Delivery Status Notification message**
 - ☞ **Message Disposition Notifications message**
 - ✓ **e.g. allow sender to see if messages have been opened**



File Transfer Protocol

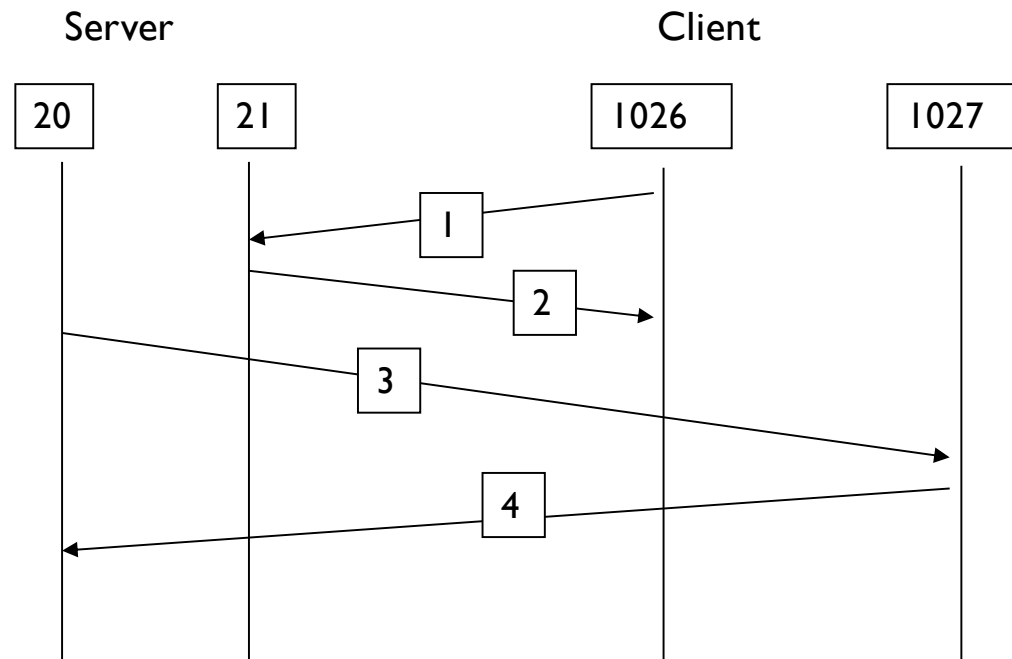


FTP

- ❑ Original specification for the FTP was written by Abhay Bhushan in 1971.
- ❑ RFC959 (published in 1985) is the current specification of FTP.
- ❑ Recent improvement
 - ☞ Security extension was proposed in RFC2229 in 1997
 - ☞ Support for IPv6 was proposed in RFC2428 in 1998
- ❑ Use separate control and data TCP connections between the client and the server
- ❑ Command response protocol
 - ☞ Similar with SMTP
 - ☞ Use ASCII code for command

Active Mode FTP

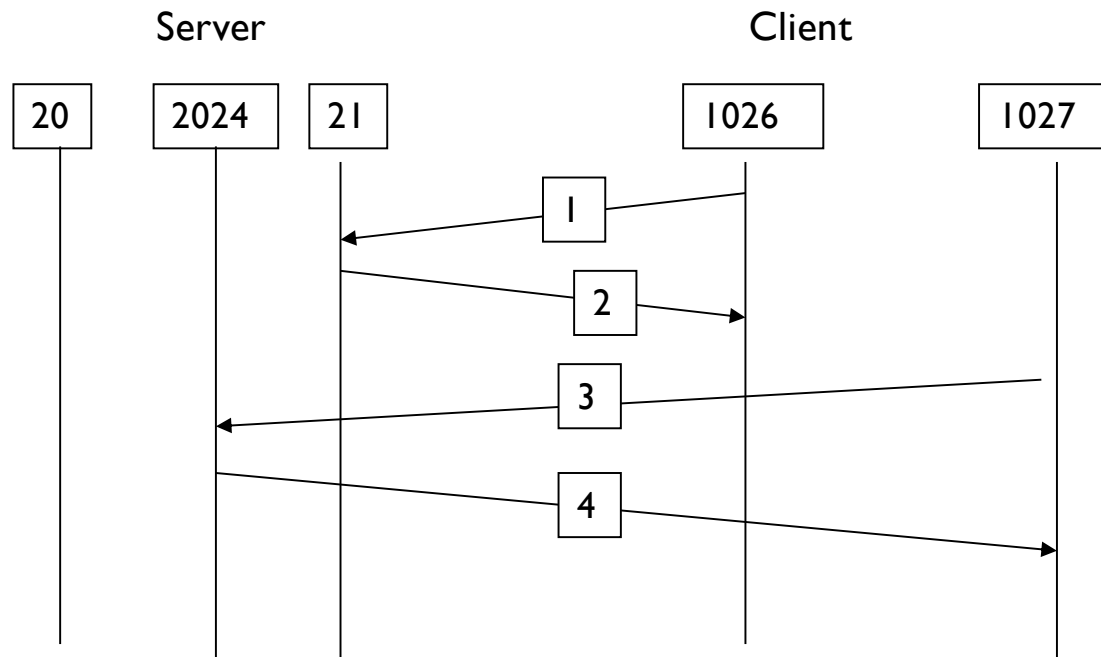
“Original” FTP, client connect from a random **unprivileged port ($n > 1023$)** to the servers command port (**21**) and sends **port command** to tell server to connect to **$n+1$** then listens on the next higher unprivileged port (**$n+1$**) for server responses. The server connects from it's data port (**20**) to the client data port (**$n+1$**)



Passive Mode FTP

“Firewall friendly FTP”

Client opens two random unprivileged ports ($n > 1023$ and $n+1$; ex 1026 and 1027) and connects the first port (n) to server command port 21 and issues a **PASV** command (server sends **port** to use for data); client connects to server's specified data port, server completes connection.



Data Transfer

❑ Data representation

- 👉 **ASCII mode:** used for plain text
- 👉 **Image mode:** used for sending binary data, byte by byte
- 👉 **EBCDIC mode:** used for sending plain text in EBCDIC character set
- 👉 **Local mode:** send data in proprietary format understandable to both sender and receiver

❑ Data transfer mode

- 👉 **Stream mode:** data is sent as a continuous stream
- 👉 **Block mode:** break data into block
- 👉 **Compressed mode:** data is compressed



Quick exercise

❑ Why **stream mode** is the most popular in FTP implementations?

- ☞ A. The stream mode is simple and easy to implement.
- ☞ B. The stream mode is scalable so that a FTP server can support many clients simultaneously.
- ☞ C. The stream mode is general since it treats all files as simple streams of bytes.
- ☞ D. The stream mode has less security vulnerabilities.

FTP Commands

- ❑ **USER** – User name, userid for access control
- ❑ **PASS** – Password for access control
- ❑ **ACCT** – Account info
- ❑ **CWD** – Change working directory
- ❑ **CDUP** – Change to parent directory
- ❑ **LS** – List files in the current remote directory
- ❑ **PUT** – Send a file to the server
- ❑ **GET** – Get a file
- ❑ **QUIT** – informs server that client wants out



Which commands will open a separate data connection?

FTP in action

```
220 FTP Server ready.  
USER ecki  
331 Password required for ecki.  
PASS youmustbekidding  
230- Linux ftp.eckenfels.net Welcome!  
230-  
230 User ecki logged in.
```

```
PASV  
227 Entering Passive Mode (212,227,90,117,5,99) # (5*256+99=1379)  
NLST  
... waiting for the data connection ...  
150 Opening ASCII mode data connection for 'file list'.  
...2 seconds to retrieve data...  
226 Transfer complete.
```

```
PORT 10, 0, 0, 1, 4, 1 # 4*256+1=1025  
200 PORT command successful.  
STOR /tmp/test.txt  
... connecting to the client ...  
150 FILE: /tmp/test.txt  
... transmitting the file ...  
226 Transfer complete.
```

Question to think

- ❑ The original design of FTP is unsecure.

```
220 FTP Server ready.  
USER ecki  
331 Password required for ecki.  
PASS youmustbekidding  
230- Linux ftp.eckenfels.net Welcome!  
230-  
230 User ecki logged in.
```

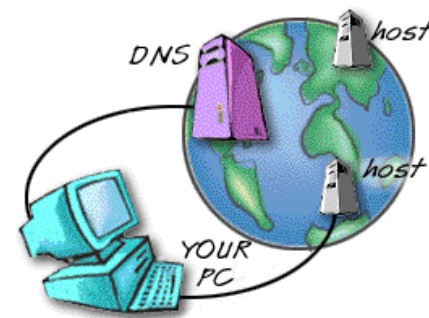
- ❑ Can we improve FTP security by encrypting user's password?

Internet Domain Name System (DNS)



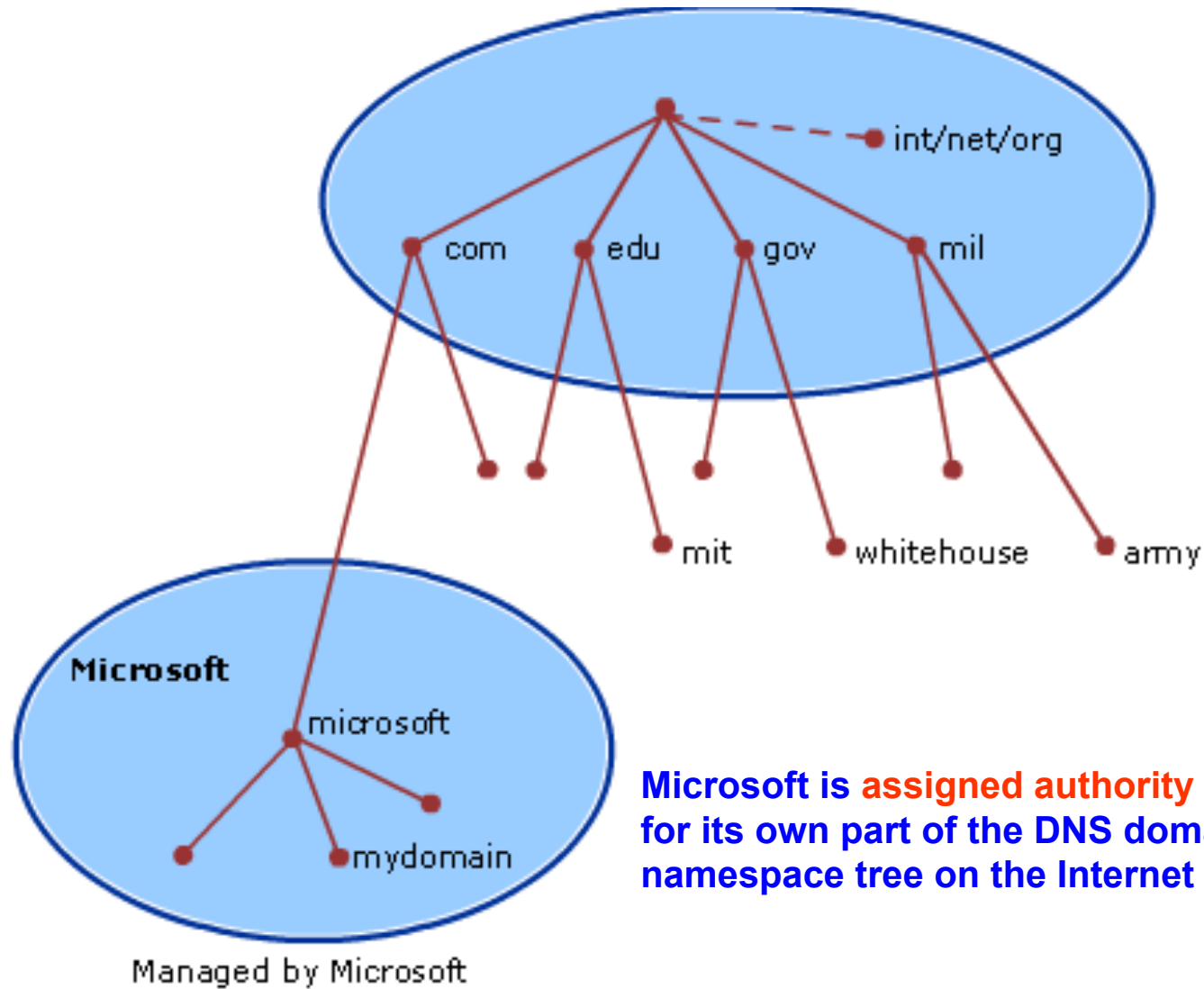
Domain Name System

- ❑ People prefer to use **names** instead of an **IP address**
- ❑ The names assigned to machines must be **unique** because the addresses are unique.
 - ☞ A name space that maps each address to a unique name can be organized in two ways: **flat** or **hierarchical**.
- ❑ The domain name space is **hierarchical** in design.
 - ☞ The names are defined in an **inverted-tree structure** with the root at the top.
 - ☞ The tree can have **128 levels: level 0 (root) to level 127**.



DNS Domain Name Hierarchy

Managed by registration authority



Some DNS Top-level Domain Names (TLDs)

DNS Domain Name	Type of Organization
com	Commercial organizations
edu	Educational institutions
org	Non-profit organizations
net	Networks (the backbone of the Internet)
gov	Non-military government organizations
mil	Military government organizations
arpa	Reverse DNS lookup
“xx”	Two-letter country code (i.e. nz, au, sg, cn, ca, etc.)



Country code

ie

India

in

Israel

it

Italy

ir

Ireland

il

Iran

Domain Names in New Zealand

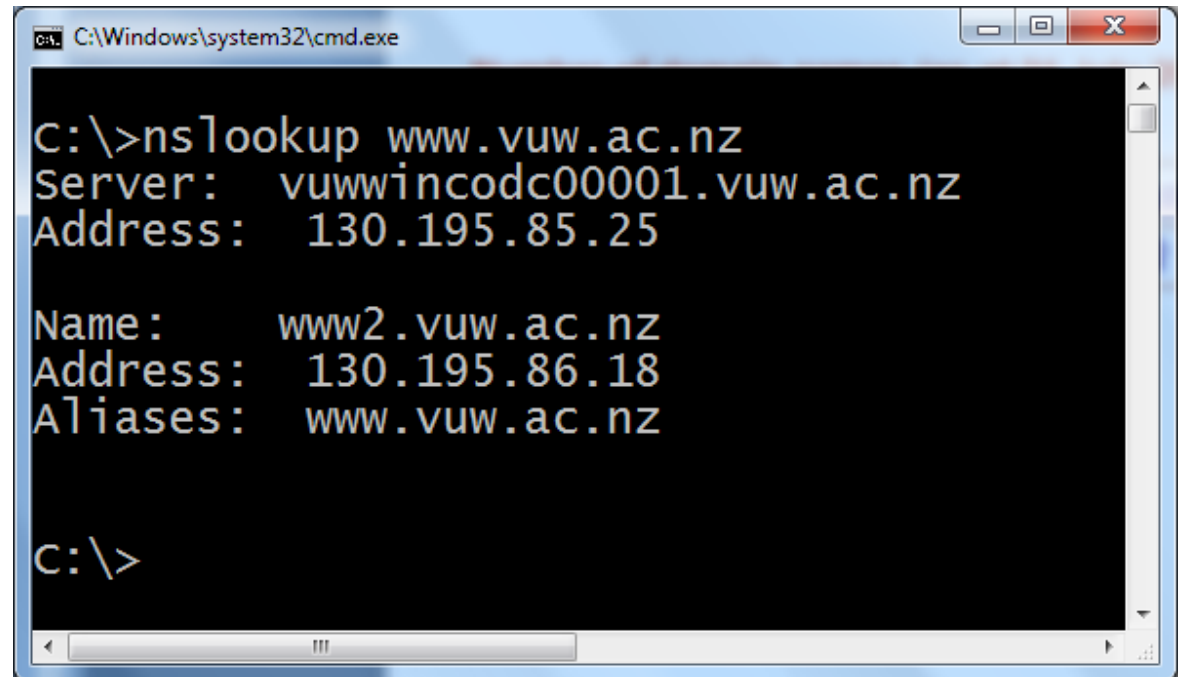
Number of domain names (July 2016 from DNC):

.ac.nz	.co.nz	.govt.nz	.health.nz	.kiwi.nz	.org.nz
2,279	483,565	1,038	231	5,240	27,940

Source: New Zealand Domain Name Commission

Use domain name service:

`nslookup www.vuw.ac.nz`



```
C:\Windows\system32\cmd.exe

C:\>nslookup www.vuw.ac.nz
Server:      vuwwincodc00001.vuw.ac.nz
Address:     130.195.85.25





Name:        www2.vuw.ac.nz
Address:     130.195.86.18
Aliases:     www.vuw.ac.nz

C:\>
```

Querying the Database

- ❑ DNS queries can be sent from a DNS client (resolver) to a DNS server, or between two DNS servers.
- ❑ A DNS query is merely a request for a specified **resource record (RR)**
 - ☞ Each **RR** identifies a particular resource within the database
 - ☞ For “**host resource**”, it contains “Owner Name (Host DNS Name) and Host IP Address”
 - ☞ For “**name server**” resource, it contains “Owner Name, Name Server DNS Name”

Quick exercise

- ☐ **DNS responses are traditionally not cryptographically signed. The _____ modifies DNS to add support for cryptographically signed responses.**
-  **A. Transport layer security**
 -  **B. Internet Name Security Extensions**
 -  **C. IPSec Extensions**
 -  **D. Domain Name System Security Extensions**

Two types of DNS queries

❑ Recursive

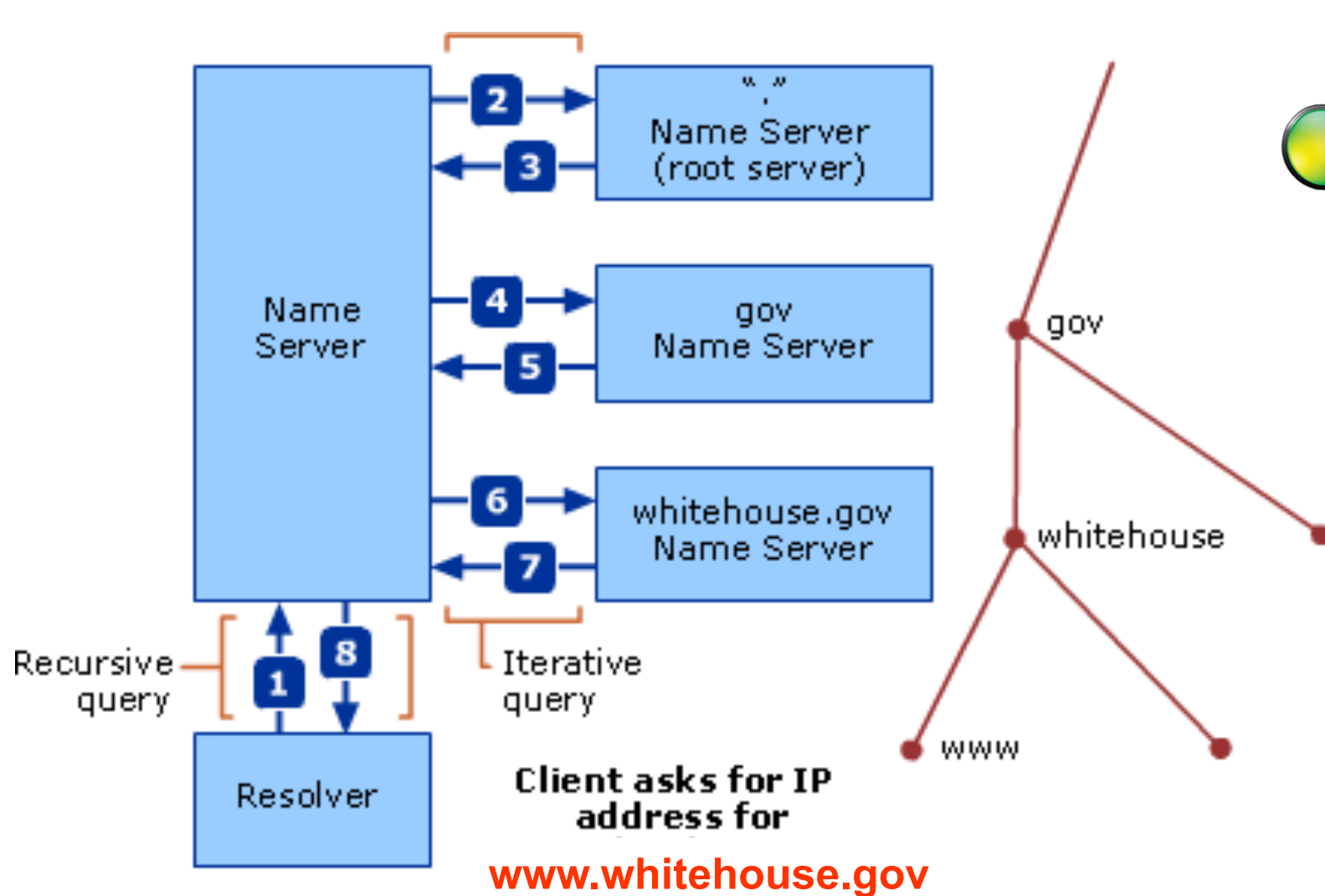
- ☞ A recursive query forces a DNS server to respond to a request with either a failure or a successful response.
- ☞ The DNS server must contact any other DNS servers it needs to resolve the request. When it receives a successful response from the other DNS server(s), it then sends a response to the DNS client.



❑ Iterative

- ☞ An iterative query is one in which the DNS server is expected to respond with the **best local information** it has
- ☞ If a DNS server does not have any local information that can answer the query, it simply sends a negative response.

How a DNS query works



Quick exercise

- ❑ What are the main drawbacks of recursive name resolution?
- ☞ A. Put higher performance demand on each name server
 - ☞ B. Communication cost is high in recursive name resolution.
 - ☞ C. Caching is less effective in recursive name resolution.
 - ☞ D. None of the above