

Computer Networking

LAB 3 – DNS

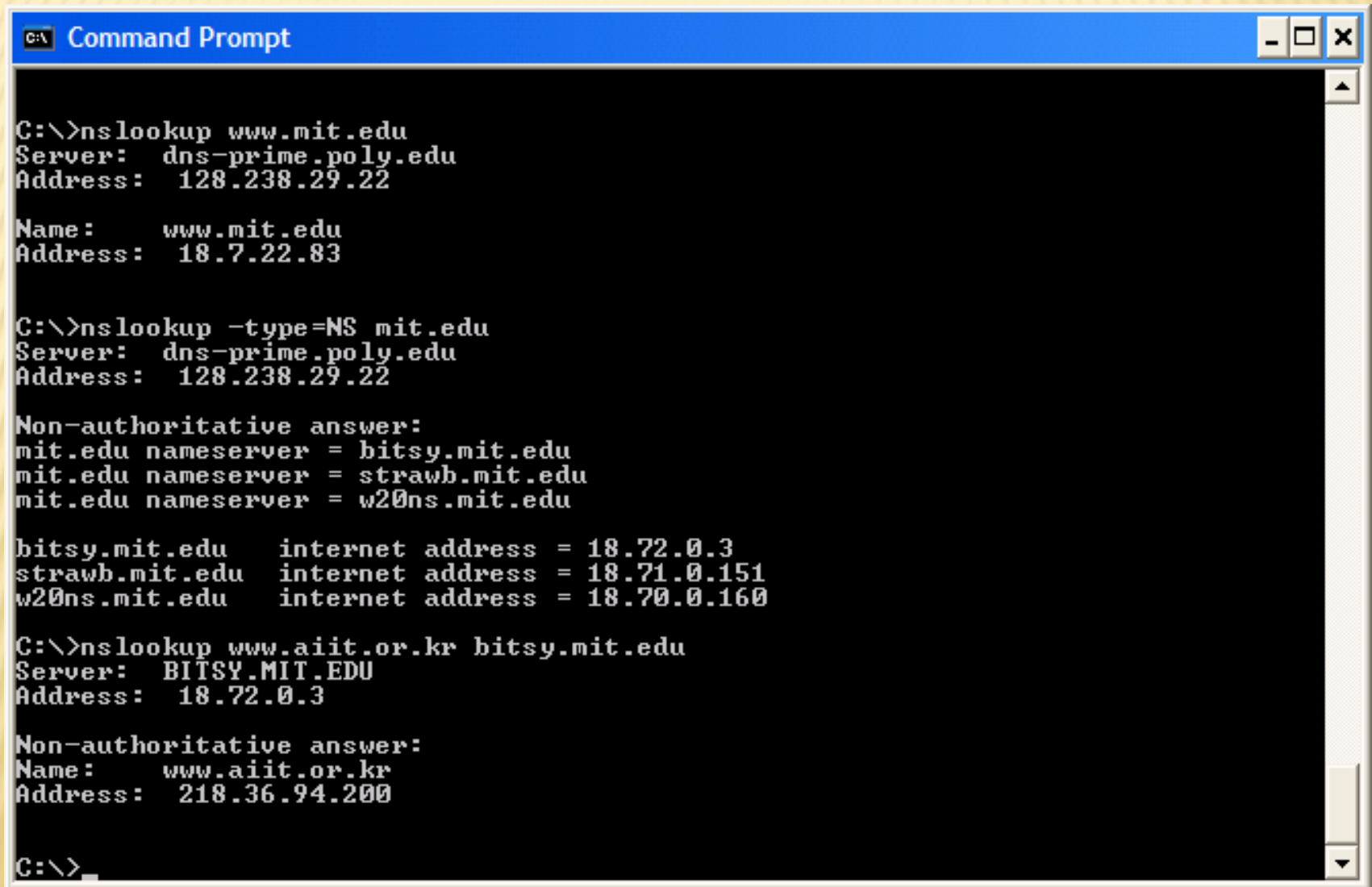
DOMAIN NAME SYSTEM

- ✖ The Domain Name System (DNS) translates hostnames to IP
- ✖ A client sends a *query* to its local DNS server, and receives a *response* back
- ✖ The hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query

1. NSLOOKUP

- ✗ *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record
- ✗ The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server

EXAMPLES



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.mit.edu
Address:  18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu   internet address = 18.71.0.151
w20ns.mit.edu    internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  218.36.94.200

C:\>
```


TEST-DRIVE

1. Run *nslookup* to obtain the IP address of a Web server in Asia
2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail

2. IPCONFIG

- ✗ used to show your current TCP/IP information, including your address, DNS server addresses, adapter type, ...
- ✗ all this information about your host:
 - + `ipconfig /all`
- ✗ useful for managing the DNS information stored in your host: `ipconfig /displaydns`
- ✗ to clear the cache: `ipconfig /flushdns`

3. TRACING DNS WITH WIRESHARK

1. Use *ipconfig* to empty the DNS cache in your host
2. Open your browser and empty your browser cache
3. Open Wireshark and enter “ip.addr == your_IP_address” into the filter
4. Start packet capture in Wireshark.
5. With your browser, visit the Web page: <http://www.ietf.org>
6. Stop packet capture

QUESTIONS

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

QUESTIONS

5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

NSLOOKUP WWW.MIT.EDU

1. What is the destination port for the DNS query message? What is the source port of DNS response message?
2. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
3. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
4. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

NSLOOKUP -TYPE=NS MIT.EDU

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
3. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

NSLOOKUP WWW.AIIT.OR.KR BITSY.MIT.EDU

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
3. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?