NANYANG TECHNOLOGICAL UNIVERSITY

CE3005: Computer Networks

Module 2-5:
Application Layer – DHCP, DNS and HTTP

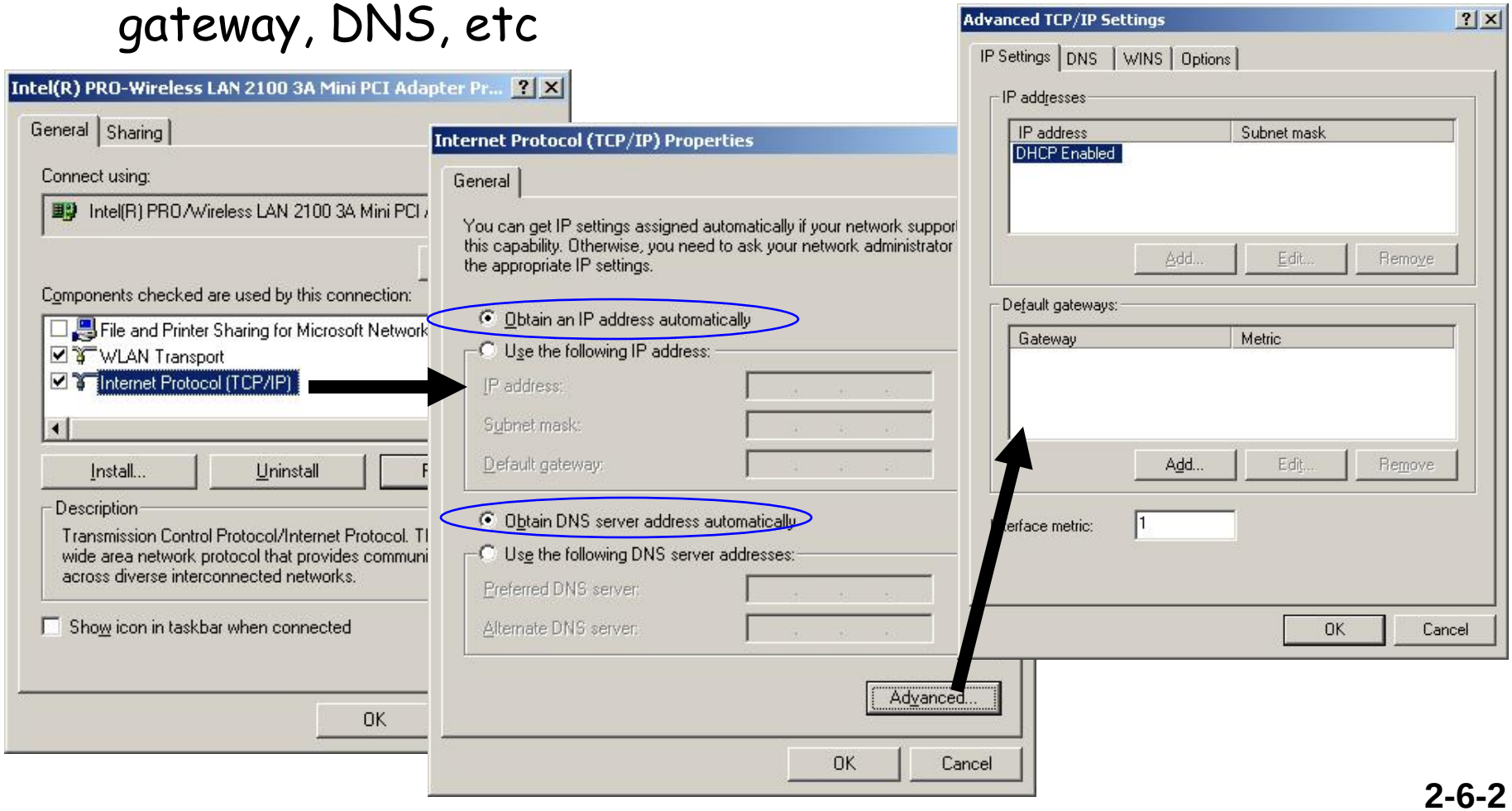
Semester 1 2016-2017

School of Computer Engineering

DHCP (RFC 2131)

Dynamic Host Configuration Protocol (DHCP)

- to automatically configure host with IP address, default gateway, DNS, etc



DHCP Protocol

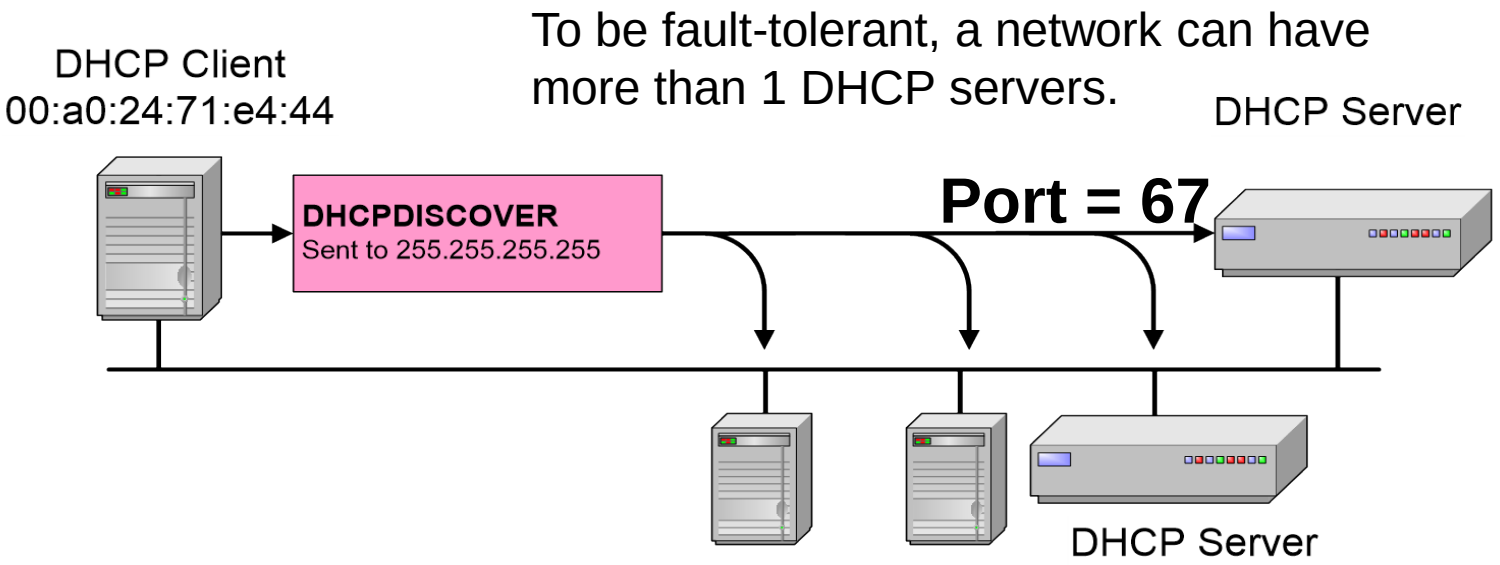
In essence, it consists of 4 steps:

1. DHCP Discover – client requesting for DHCP server
2. DHCP Offer – server responding to client's request
3. DHCP Request – client accepting server's offer
4. DHCP Acknowledge – server confirming the offer

- DHCP protocol is designed to run over UDP with server listening at well-known port 67.
- Instead of ephemeral port, DHCP is an exception where client is required to run at well-known port 68.

Why? [Read RFC 951]

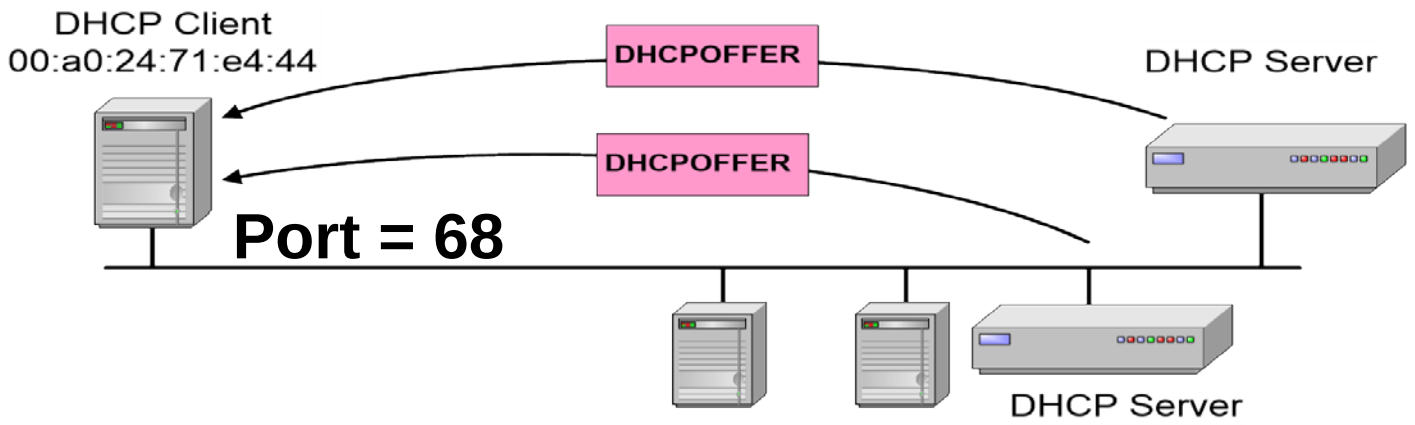
DHCP Discover



- Host/DHCP client sends DHCP Discover message to destination address 255.255.255.255 (IP broadcast) since it does not know where the server is.
- Client uses source IP address 0.0.0.0 since it does not have an IP address.
- If client is able to receive unicast DHCP reply even without an IP address, set DHCP message broadcast flag = 0. Otherwise, set it to 1.

DHCP Offer

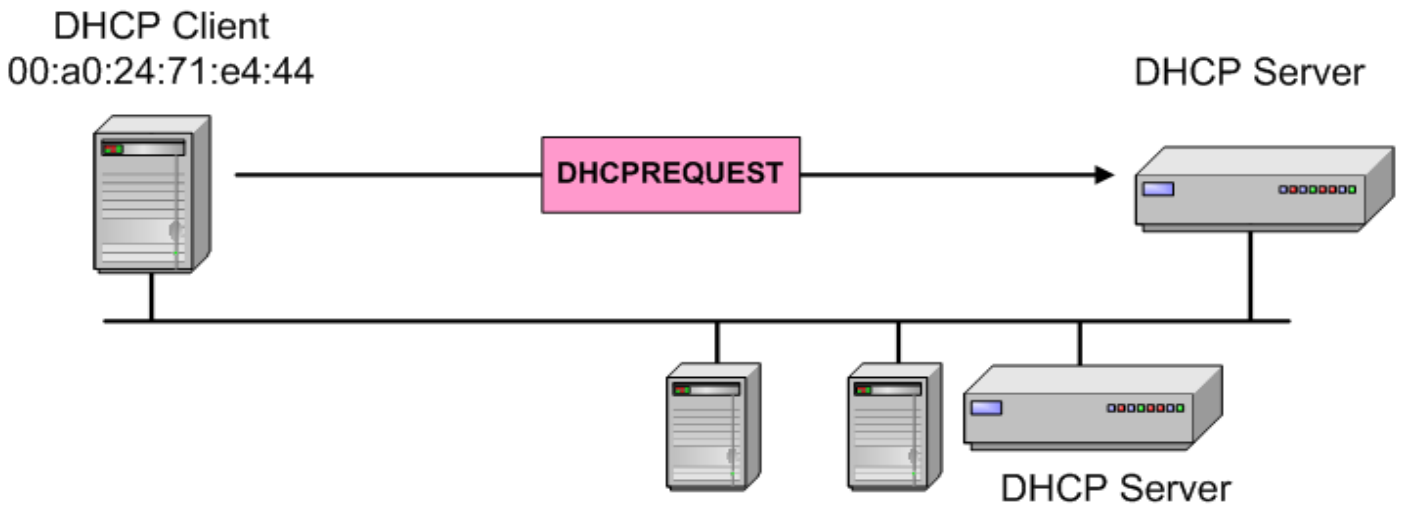
Both DHCP servers can respond with offers.



- Based on received DHCP message broadcast flag, DHCP servers send DHCP Offer via:
  - IP unicast using offered IP as destination address (possible since client's physical address is known); or
  - IP broadcast to destination address 255.255.255.255
- Reason why client is not using ephemeral port:

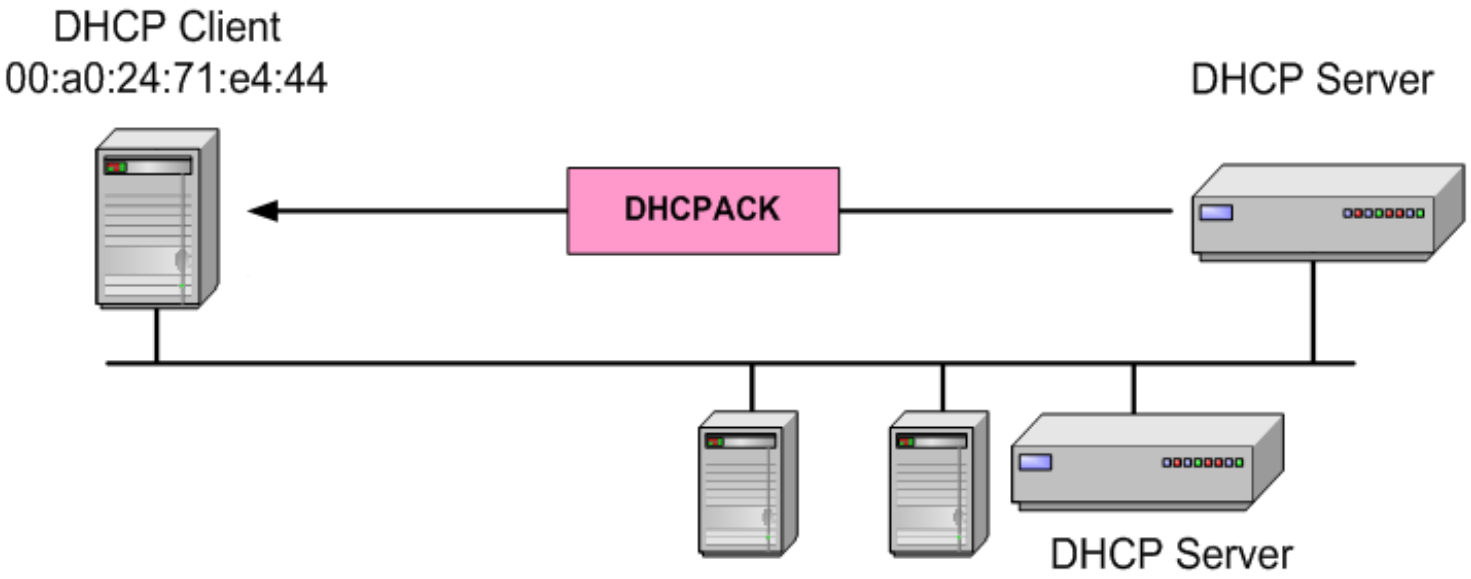
  ➢ Could confuse other hosts which happened to be using the same UDP ephemeral port as the DHCP client if IP broadcast is used.

DHCP Request



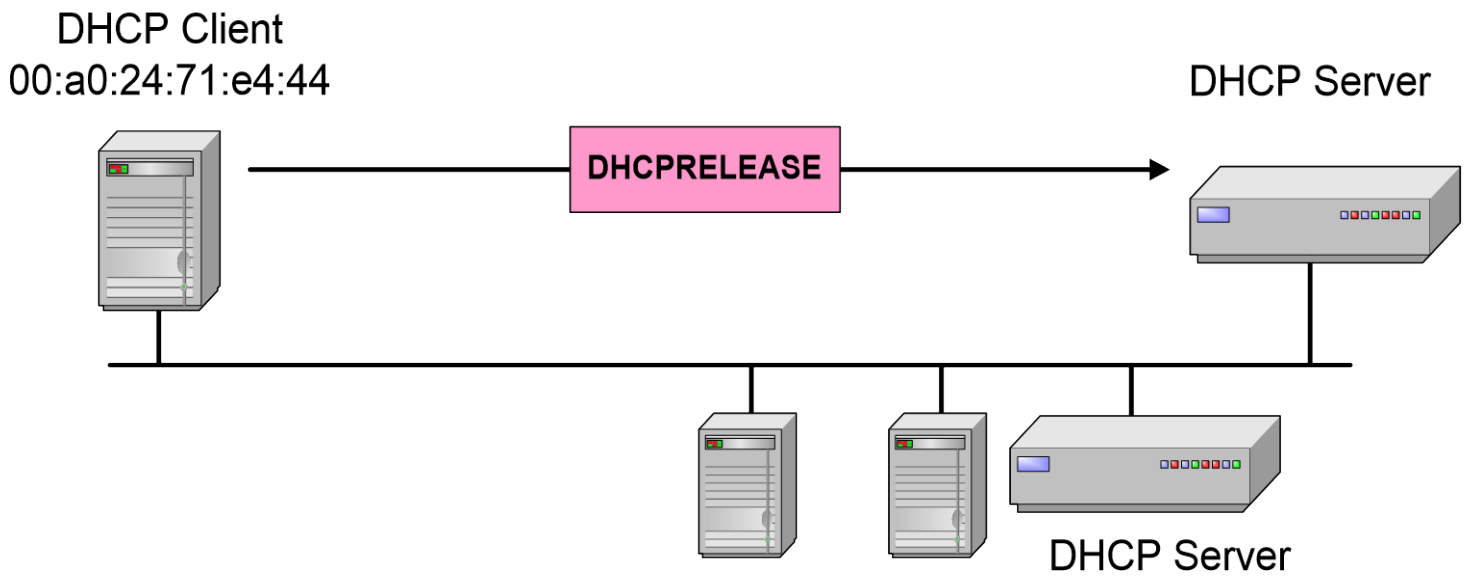
- Client selects one offer and sends DHCP Request which includes the selected server identifier.
- DHCP Request is sent to destination address 255.255.255.255 (IP broadcast) so that other DHCP servers will also receive it and know that their offers are being declined.
- Client still uses source IP 0.0.0.0 since the offer is not confirmed yet.

DHCP Acknowledge



- Similar as DHCP Offer, DHCP Ack is sent via IP unicast or broadcast based on the DHCP message broadcast flag.
- Once DHCP Ack is received, the client can start using the offered IP address within the duration of the lease time, typically 1 day.

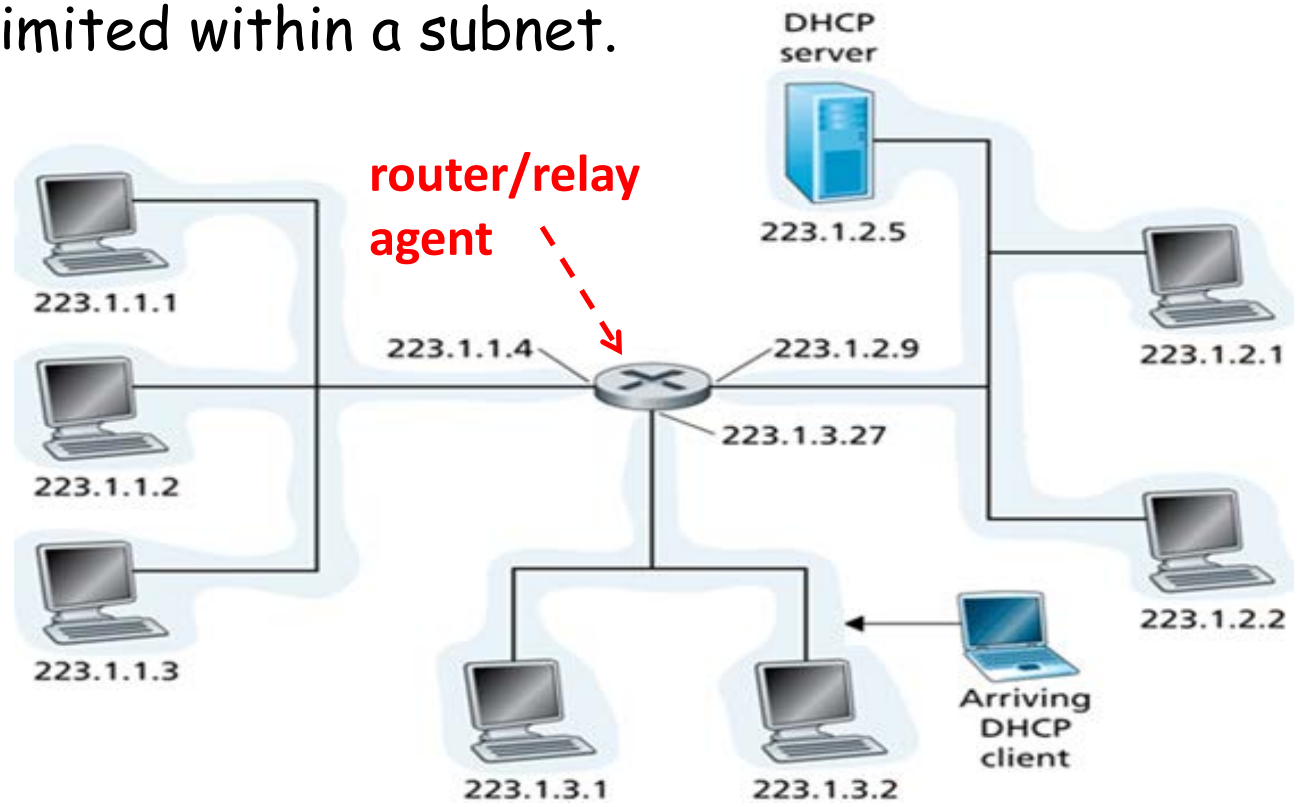
DHCP Release



- To extend the lease, the process of DHCP Request/Ack is repeated.
- To end the lease, the client sends DHCP Release via unicast to the server.

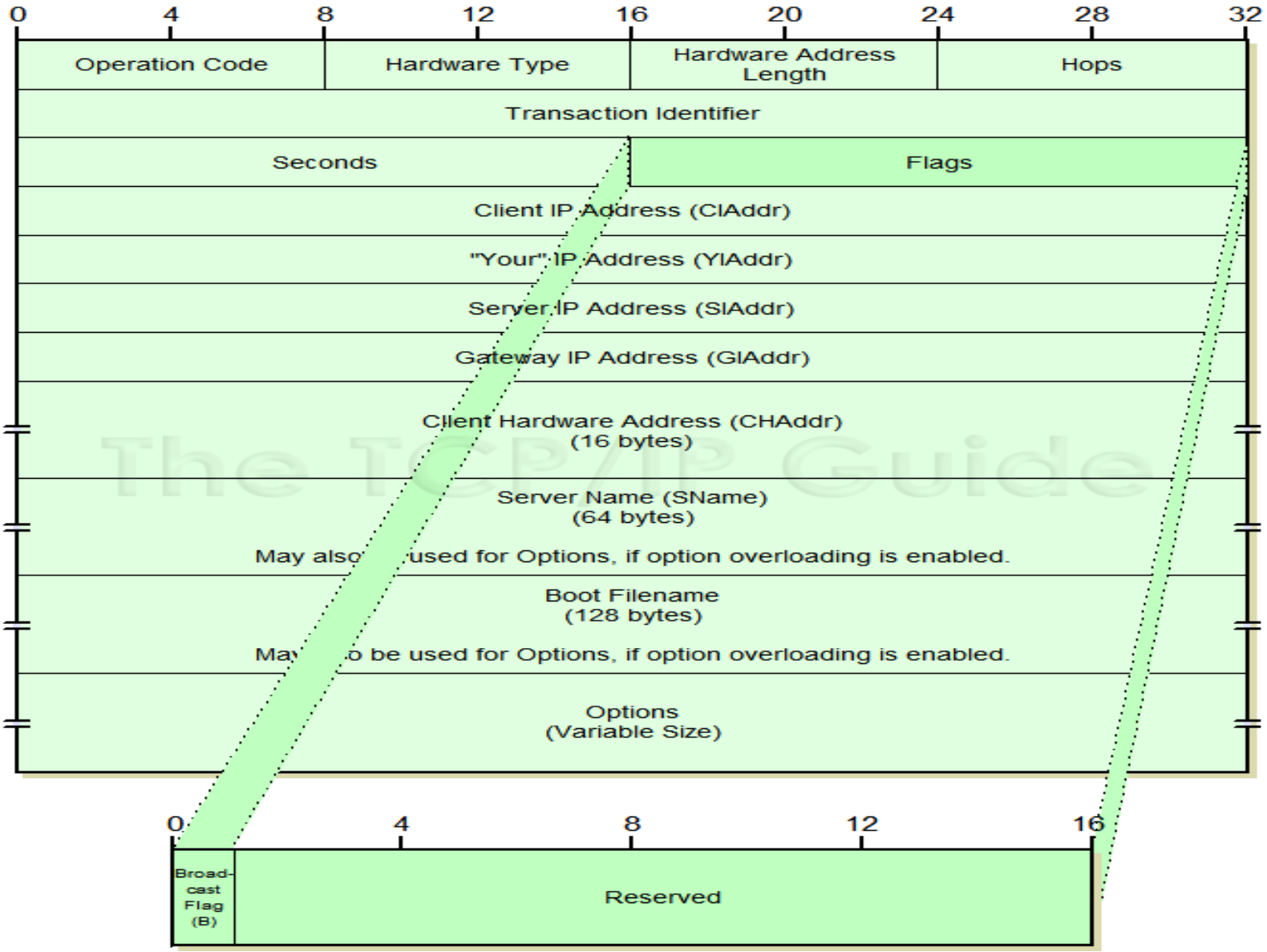
DHCP Relay Agent

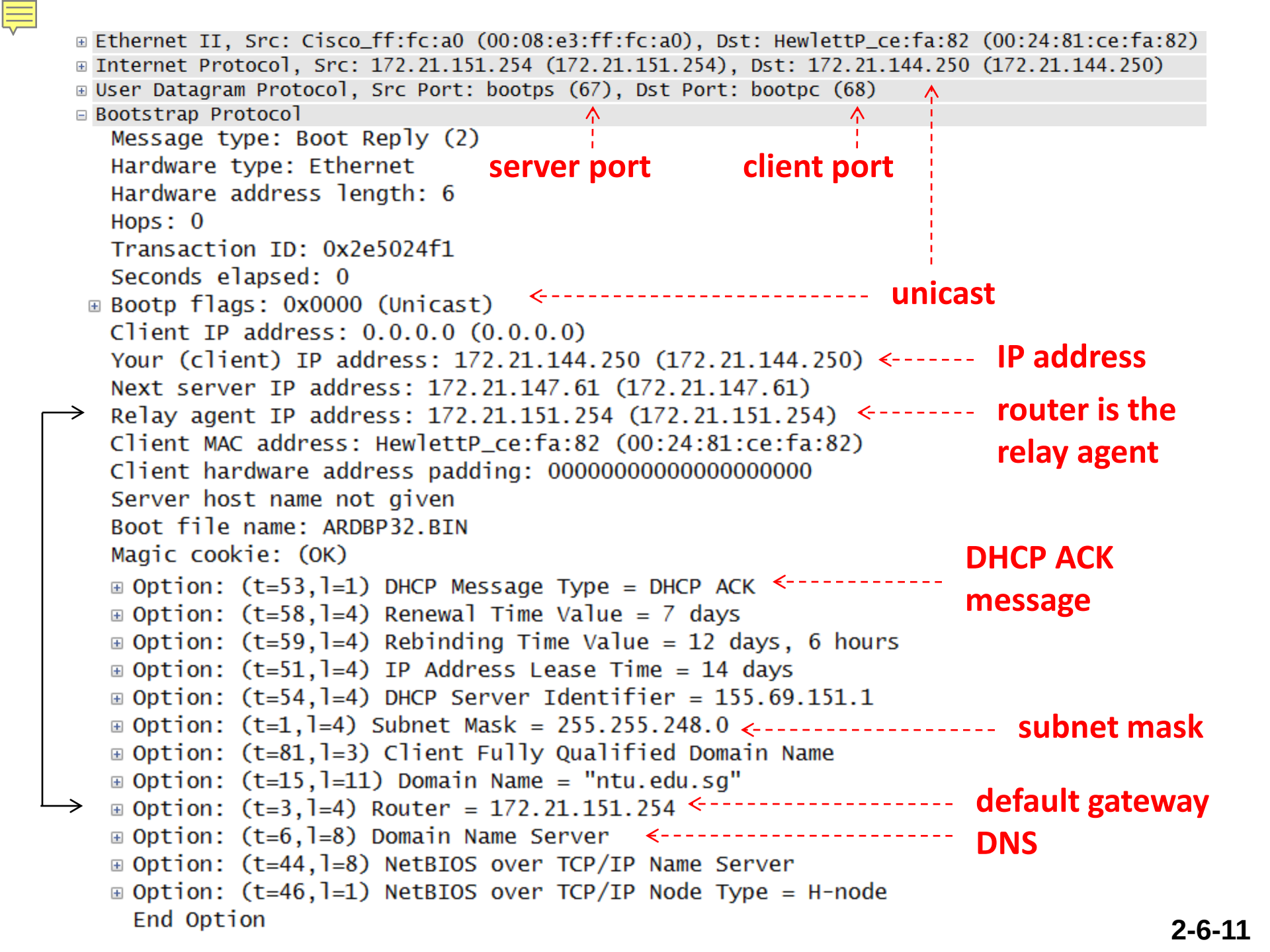
To enable DHCP server to support multiple subnets, relay agents are required since IP broadcast 255.255.255.255 is only limited within a subnet.



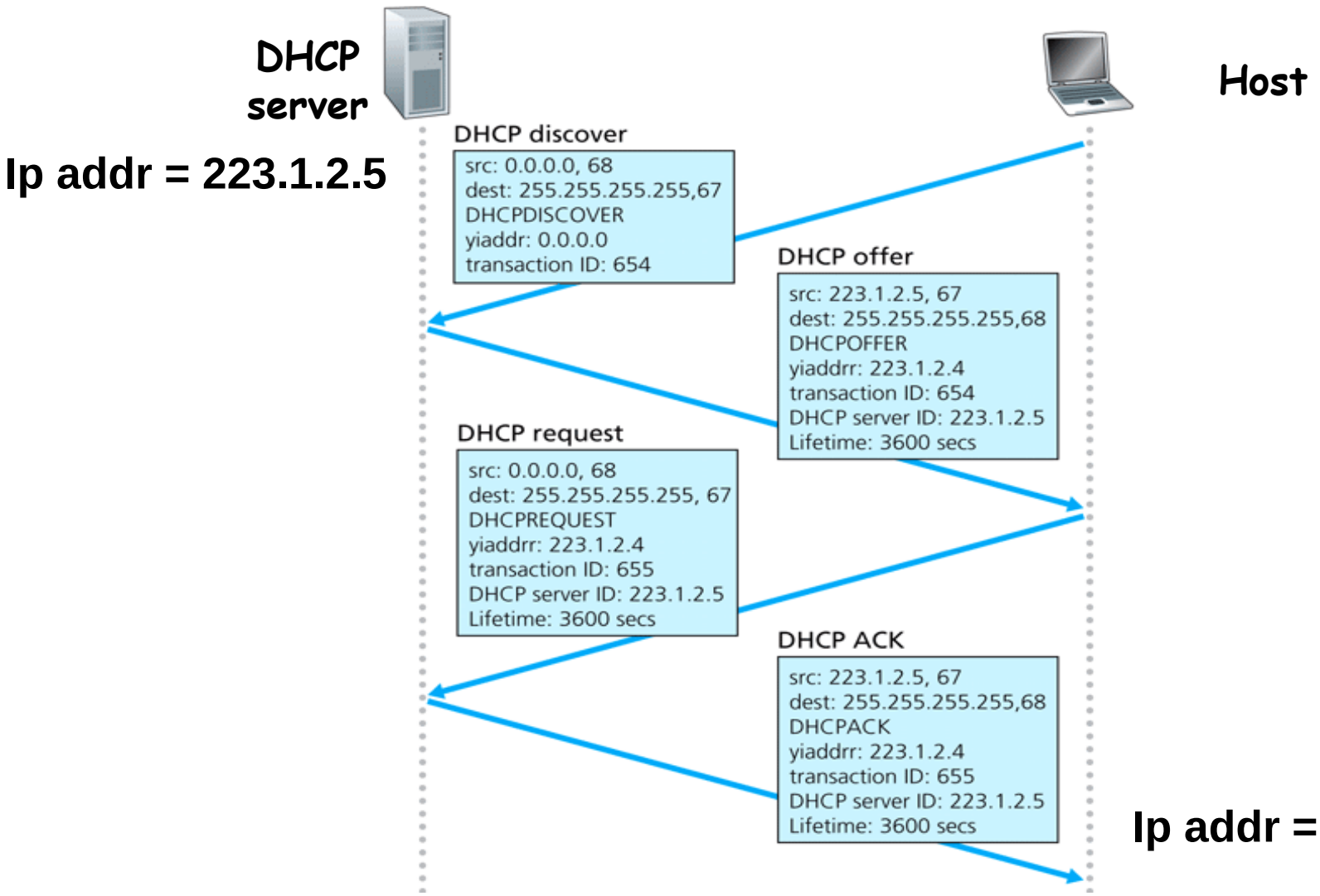
To save the trouble of having dedicated relay agent in every subnet, some routers have the added functionality to act as relay agents.

DHCP Message Format



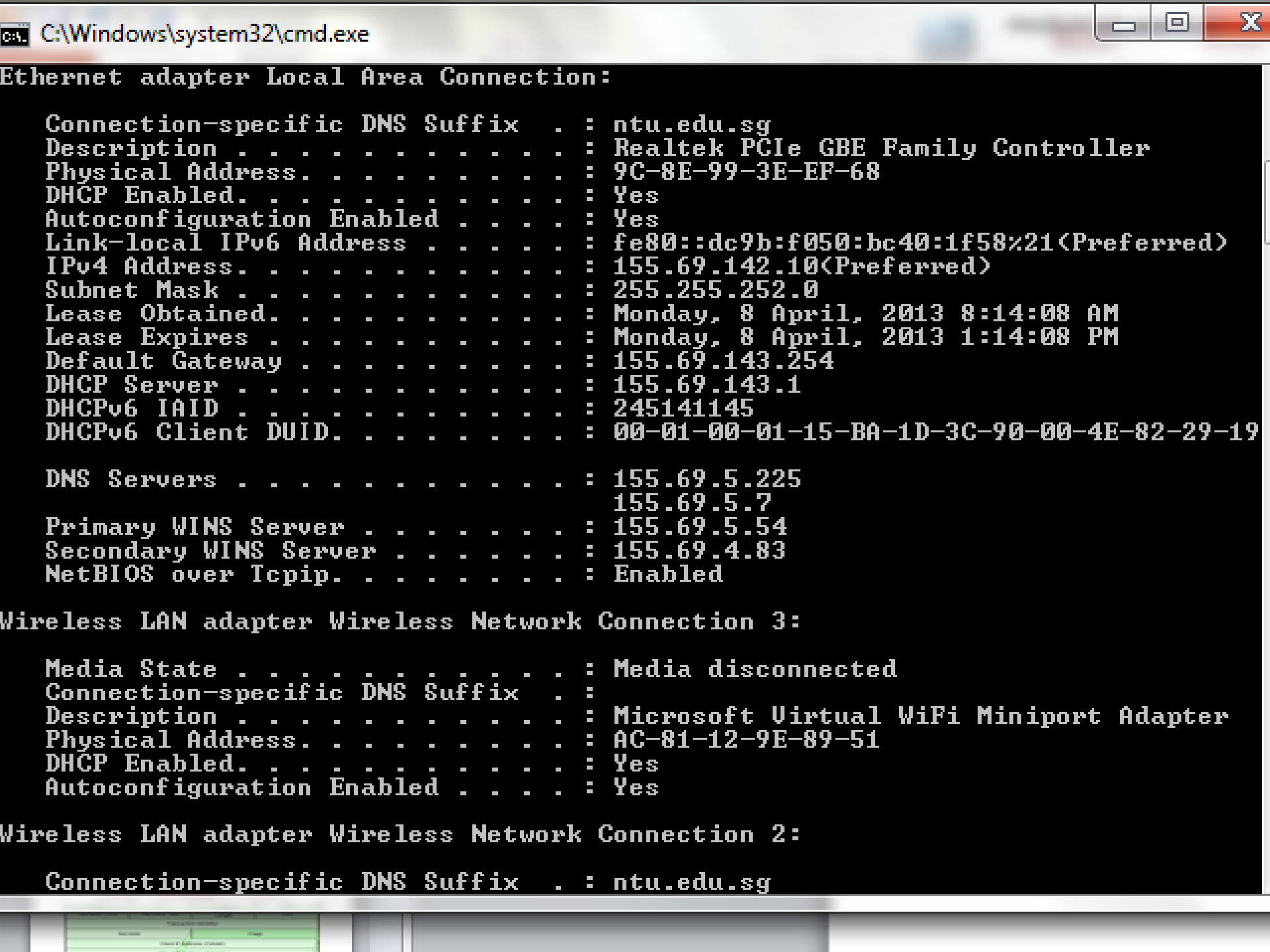

Ethernet II, Src: Cisco_ff:fc:a0 (00:08:e3:ff:fc:a0), Dst: HewlettP_ce:fa:82 (00:24:81:ce:fa:82)
Internet Protocol, Src: 172.21.151.254 (172.21.151.254), Dst: 172.21.144.250 (172.21.144.250)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x2e5024f1
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 172.21.144.250 (172.21.144.250)
Next server IP address: 172.21.147.61 (172.21.147.61)
Relay agent IP address: 172.21.151.254 (172.21.151.254)
Client MAC address: HewlettP_ce:fa:82 (00:24:81:ce:fa:82)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name: ARDBP32.BIN
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=58,l=4) Renewal Time Value = 7 days
Option: (t=59,l=4) Rebinding Time Value = 12 days, 6 hours
Option: (t=51,l=4) IP Address Lease Time = 14 days
Option: (t=54,l=4) DHCP Server Identifier = 155.69.151.1
Option: (t=1,l=4) Subnet Mask = 255.255.248.0
Option: (t=81,l=3) Client Fully Qualified Domain Name
Option: (t=15,l=11) Domain Name = "ntu.edu.sg"
Option: (t=3,l=4) Router = 172.21.151.254
Option: (t=6,l=8) Domain Name Server
Option: (t=44,l=8) NetBIOS over TCP/IP Name Server
Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = H-node
End Option
server port
client port
unicast
IP address
router is the relay agent
DHCP ACK message
subnet mask
default gateway
DNS

Then, ISPs/organizations may allocate IP address to individual host by manual configuration or automatically by Dynamic Host Configuration Protocol (DHCP).



Basic Information

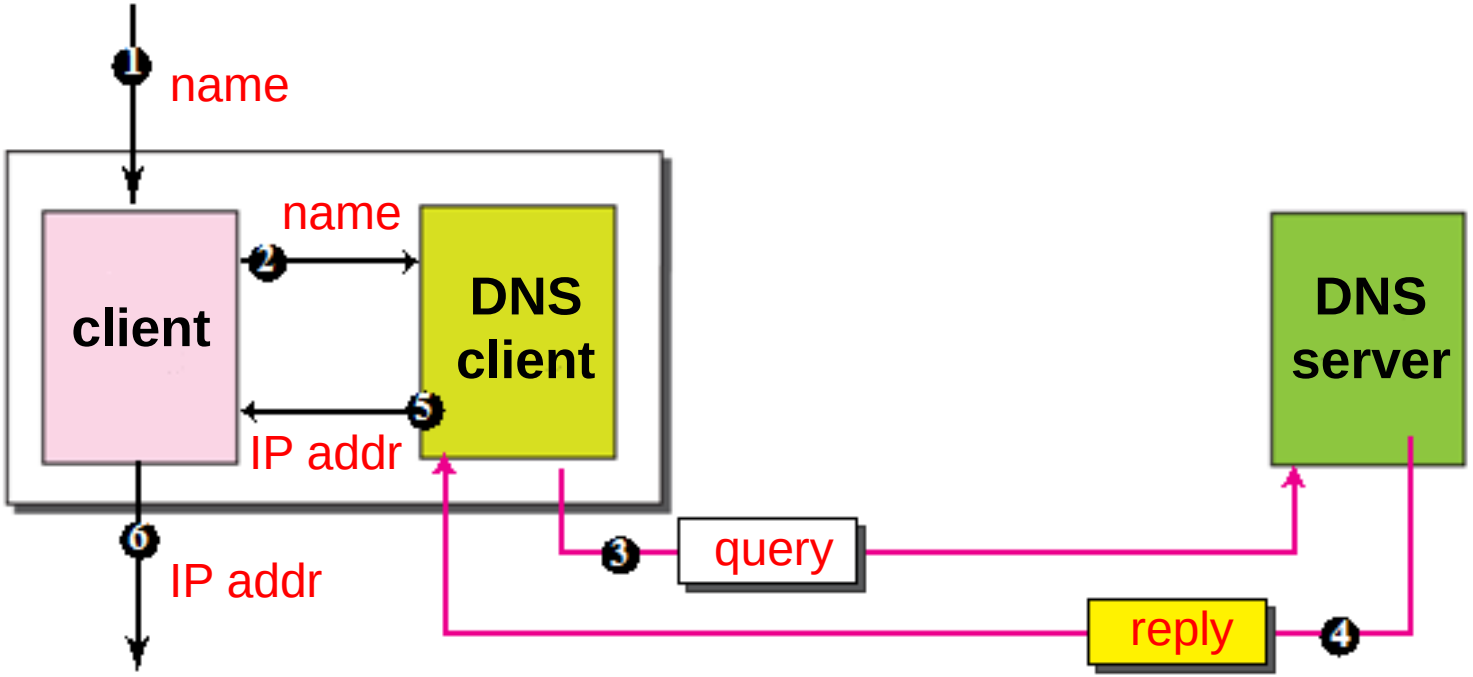
- **IP address for client**
- **Subnet mask**
- **Default gateway**
- **DNS**
- ***WINS**


C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : ntu.edu.sg
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 9C-8E-99-3E-EF-68
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::dc9b:f050:bc40:1f58%21(Preferred)
IPv4 Address. . . . . : 155.69.142.10(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : Monday, 8 April, 2013 8:14:08 AM
Lease Expires . . . . . : Monday, 8 April, 2013 1:14:08 PM
Default Gateway . . . . . : 155.69.143.254
DHCP Server . . . . . : 155.69.143.1
DHCPv6 IAID . . . . . : 245141145
DHCPv6 Client DUID. . . . . : 00-01-00-01-15-BA-1D-3C-90-00-4E-82-29-19
DNS Servers . . . . . : 155.69.5.225
155.69.5.7
Primary WINS Server . . . . . : 155.69.5.54
Secondary WINS Server . . . . . : 155.69.4.83
NetBIOS over Tcpip. . . . . : Enabled
Wireless LAN adapter Wireless Network Connection 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter
Physical Address. . . . . : AC-81-12-9E-89-51
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wireless Network Connection 2:
Connection-specific DNS Suffix . : ntu.edu.sg

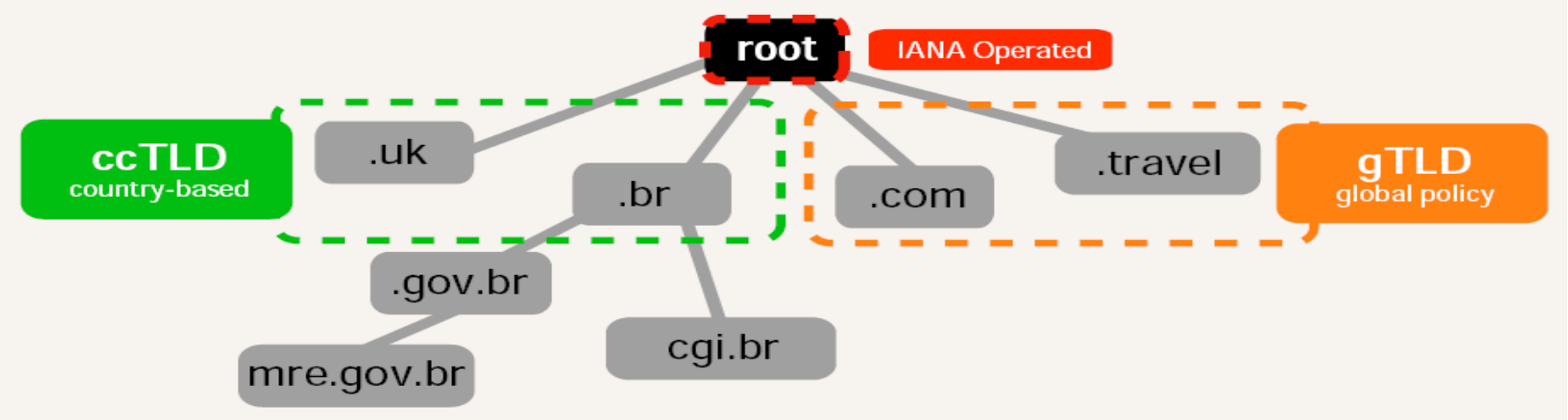
Domain Name System (DNS)

Given only the domain name of a server, how does a client know the IP address to send to destination?

- DNS – to resolve domain name to IP address



- DNS protocol is designed to run over UDP with server listening at well-known port 53.



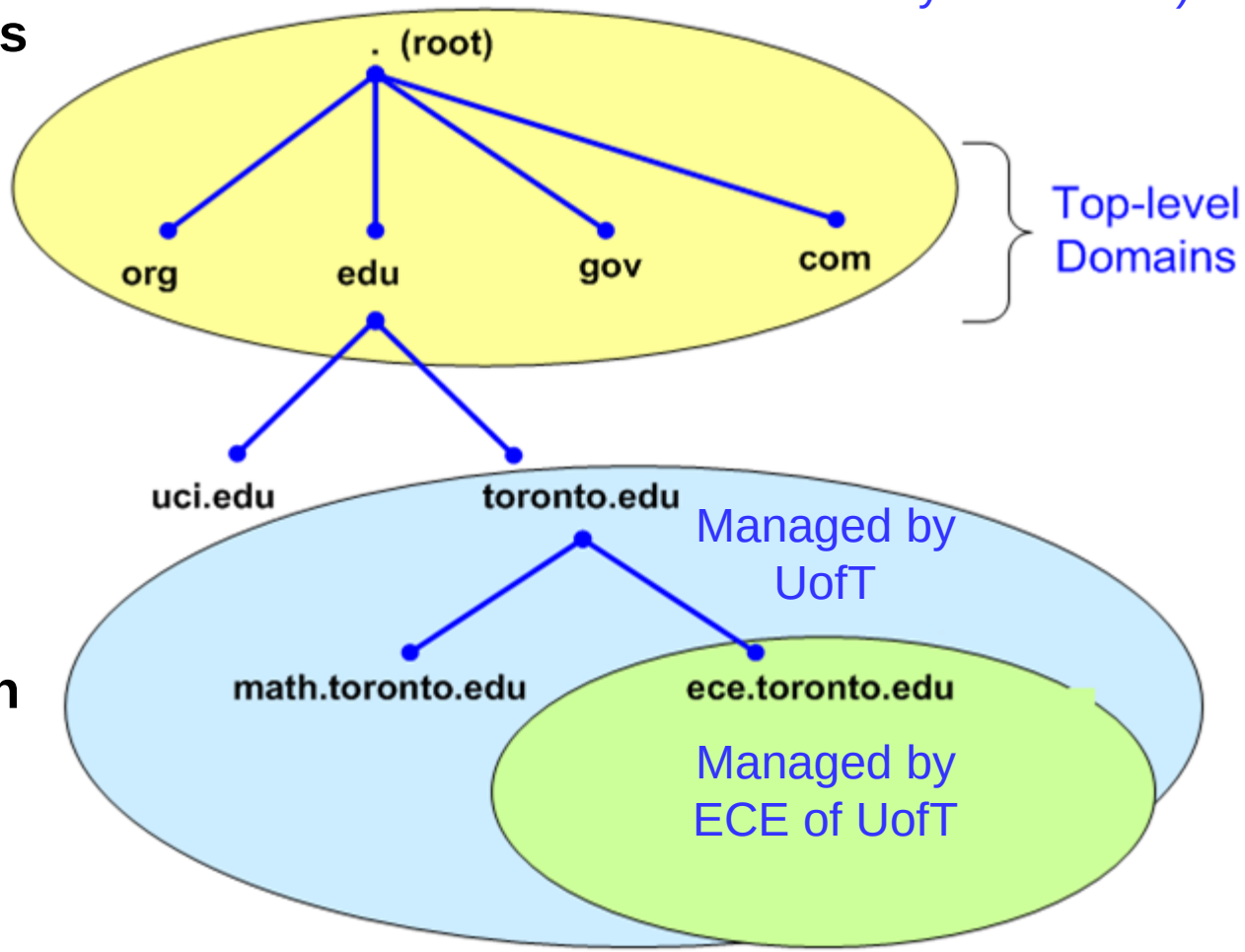
Domain names are divided into gTLDs and ccTLDs, and commercial domain name registrars are accredited to sell them:

- generic Top-Level Domains (gTLDs): only IANA/ICANN-accredited registrars are able to sell domain names under gTLDs
- country-code Top-Level Domains (ccTLDs): delegated to respective countries, e.g. only (Singapore) SGNIC-accredited registrars can sell domain names under .sg

For scalability, domain names are designed to be hierarchical; e.g. ece.toronto.edu.

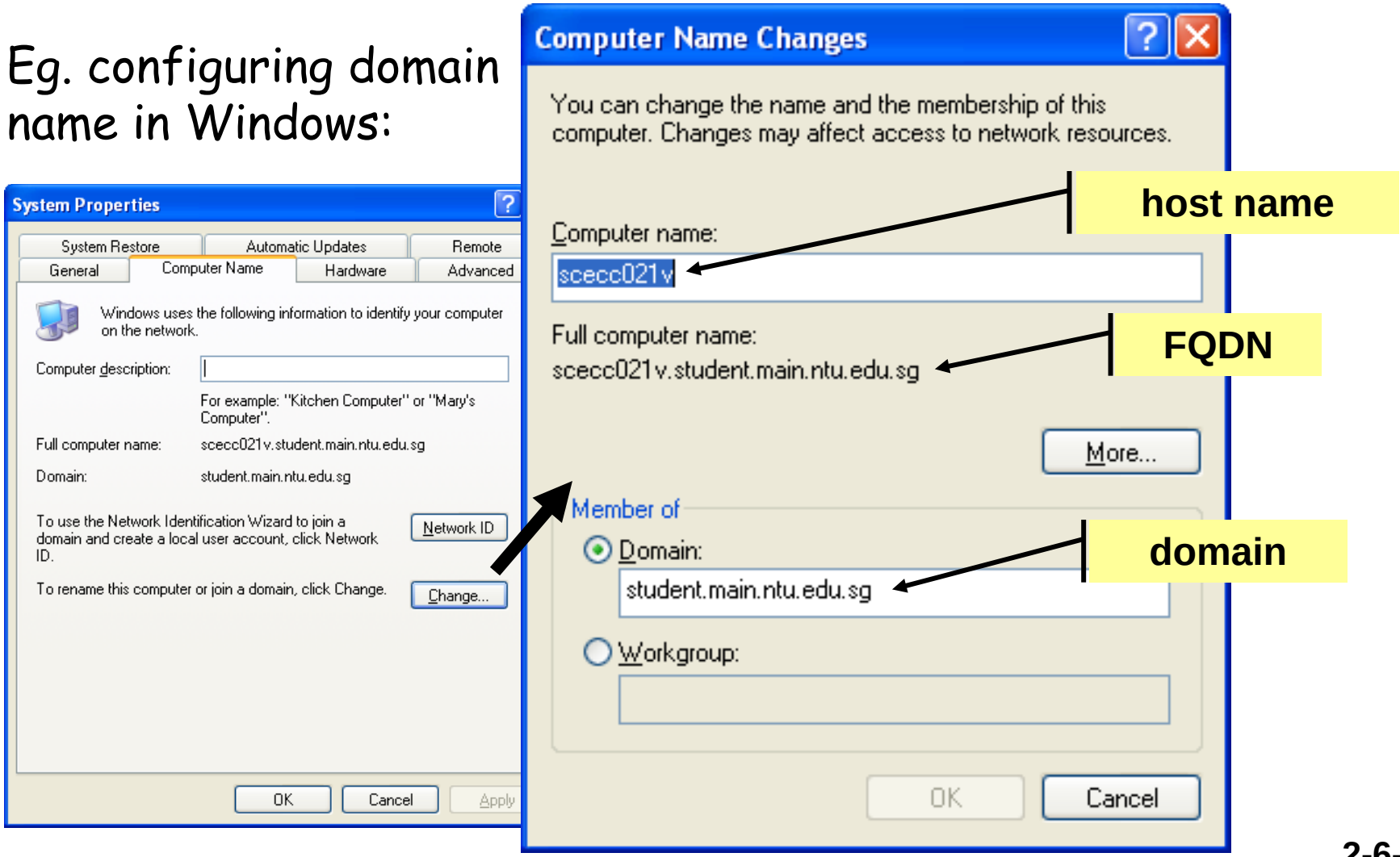
3rd level 2nd level top level root (last dot may be omitted)

- **Top-level domains are managed by IANA**
- **Below top-level domains, management of name space is delegated to respective organizations**
- **Each organization can delegate further**



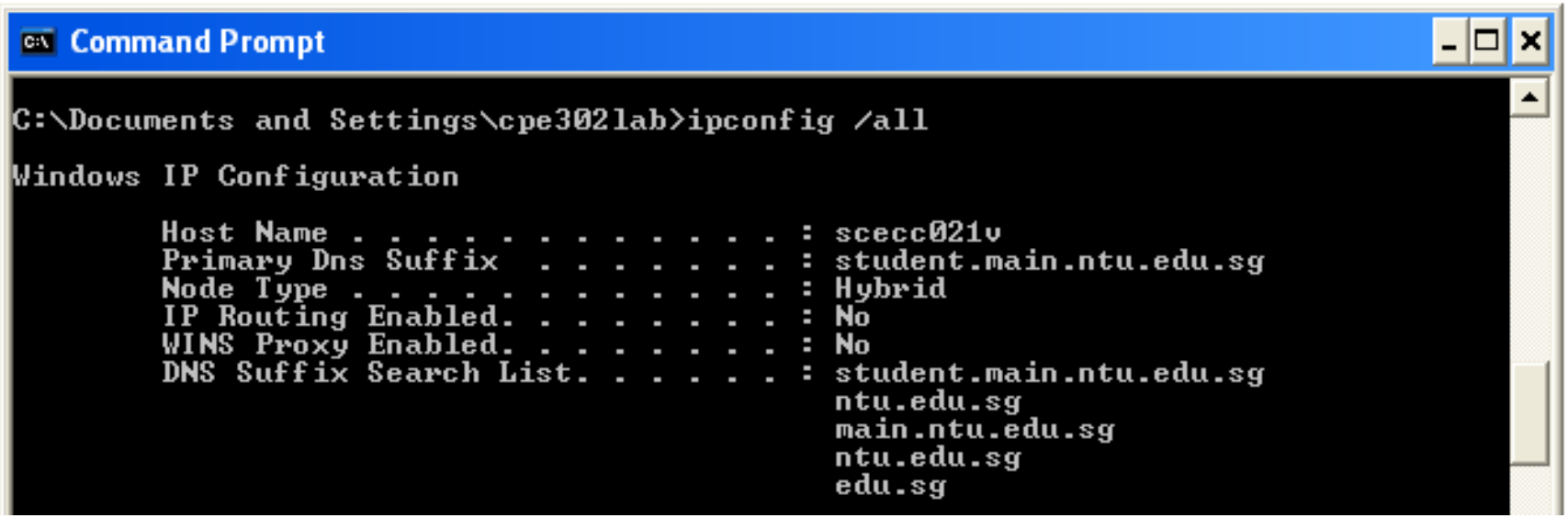
A fully qualified domain name (FQDN) is a completely specified domain name consisting of a host name and a domain.

Eg. configuring domain name in Windows:



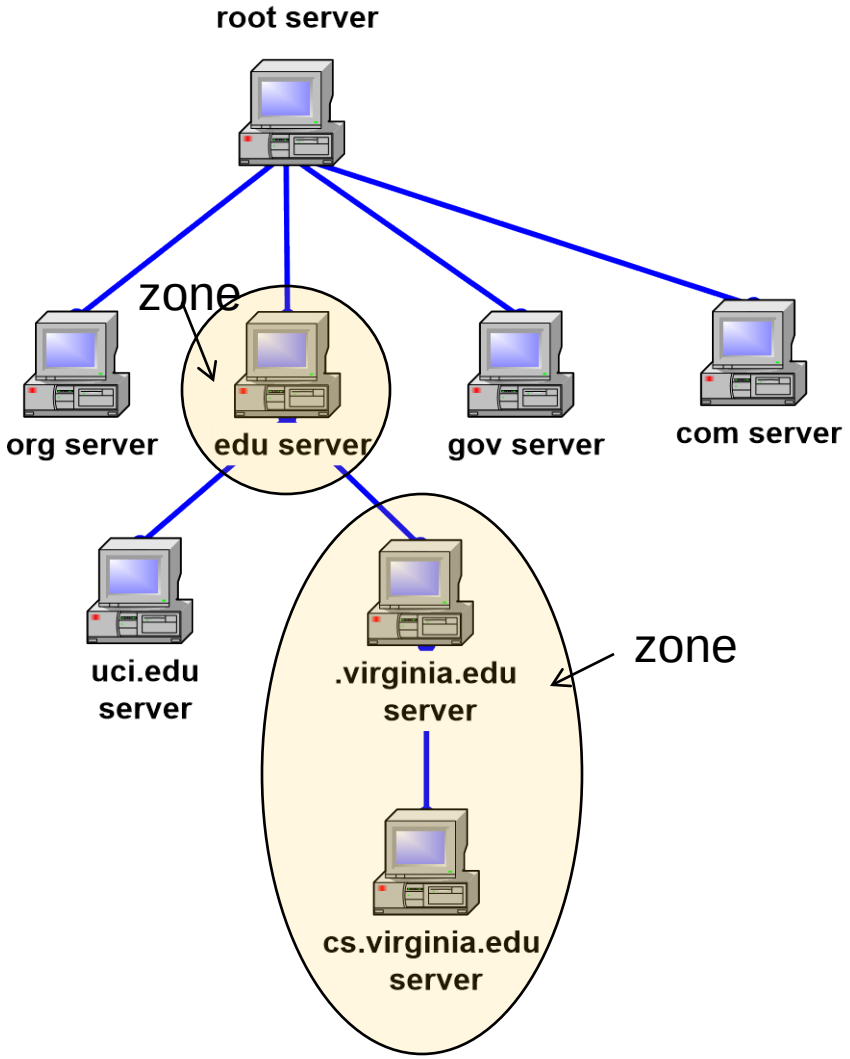
If given just the host name, a DNS resolver may attempt to resolve it by appending appropriate domains based on configuration.

Eg. in Windows, the DNS Suffix Search List specifies the domains that a resolver should try if given only the host name.



Following the hierarchy of domain names, a hierarchy of name servers are set up to provide DNS services.

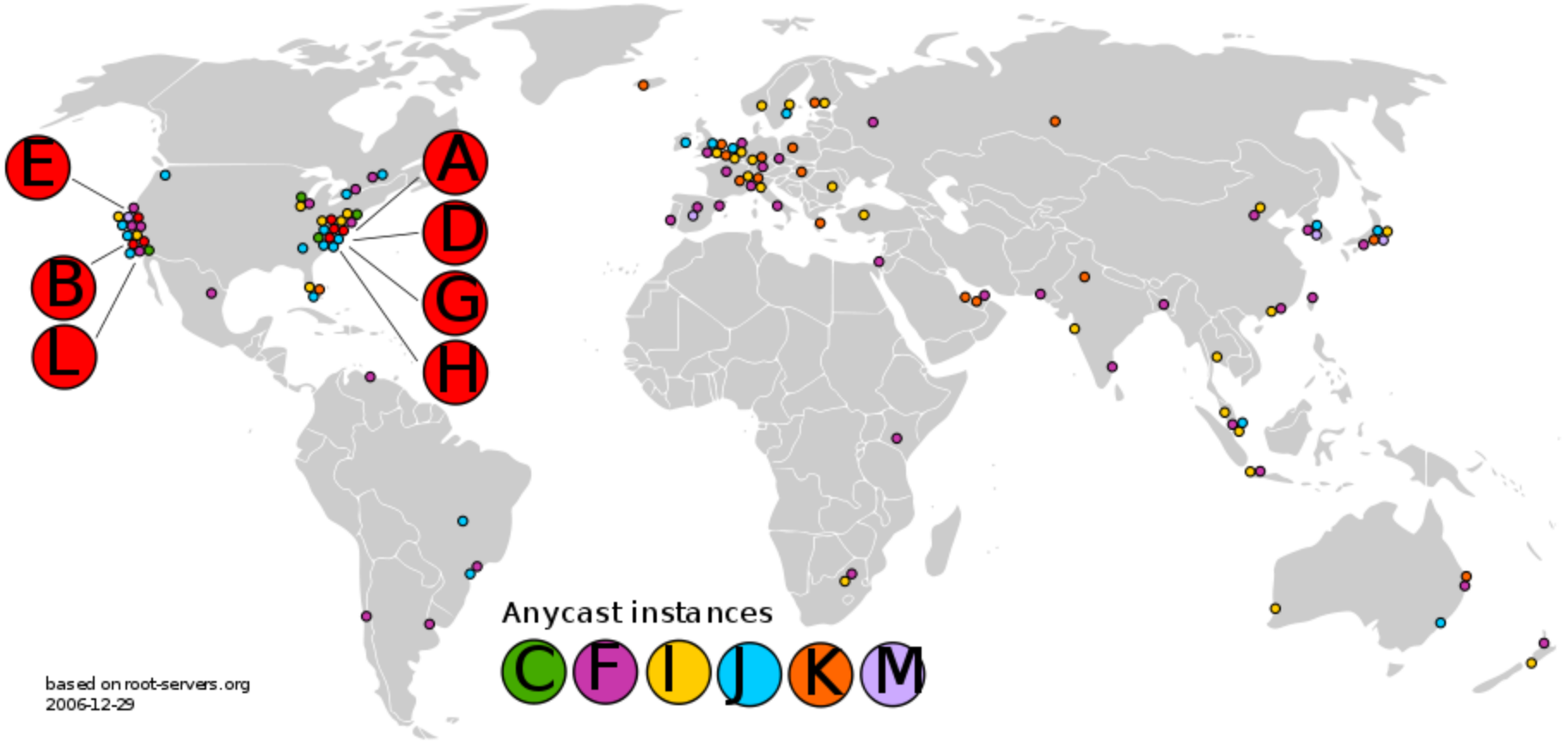
- **Each server is responsible (authoritative) for a zone of the DNS namespace.**
- **A zone can be a node; e.g. edu server is authoritative for *xxx.edu***
- **A zone can also consist of multiple nodes; e.g. virginia.edu server is authoritative for *xxx.virginia.edu*, including *xxx.cs.virginia.edu***



To be fault tolerant, there are 13 root name servers which are configured to know the authoritative servers for TLDs.

Domain Name	Operator	IP Address
a.root-servers.net	VeriSign	198.41.0.4
b.root-servers.net	USC-ISI	192.228.79.201
c.root-servers.net	Cogent Communications	192.33.4.12
d.root-servers.net	University of Maryland	128.8.10.90
e.root-servers.net	NASA	192.203.230.10
f.root-servers.net	Internet Systems Consortium	192.5.5.241
g.root-servers.net	US DoD	192.112.36.4
h.root-servers.net	US Army Research Lab	128.63.2.53
i.root-servers.net	Autonomica Stockholm	192.36.148.17
j.root-servers.net	VeriSign	192.58.128.30
k.root-servers.net	RIPE London	193.0.14.129
l.root-servers.net	ICANN Los Angeles	199.7.83.42
m.root-servers.net	WIDE Tokyo	202.12.27.33

In reality, there are more than 13 physical root name servers through the use of anycast.



Anycast – a group of servers are identified by the same IP address, and packets are routed to the nearest servers


Map
Satellite
Hybrid
Greenland
Iceland
Canada
North Atlantic Ocean
México
Venezuela
Perú
Bolivia
Brazil
Argentina
South Atlantic Ocean
Suomi Finland
Norge Norway
Россия Russia
Kazakhstan
Mongolia
China
S.Korea
Japan
North Pacific Ocean
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Saudi Arabia
Iraq
DR Congo
Kenya
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
Southern Ocean
Legend
Multiple instances
Single instance
POWERED BY Google
Map data ©2009 Europa Technologies - Terms of Use

Security

In Security:
News
Reviews
Features
How-tos
Slideshows

China suffers major DDoS attack on .cn domain

It's still unclear where the DDoS attack originated from

By Michael Kan | Published: 11:21, 26 August 2013

China's Internet on early Sunday morning suffered a major distributed denial of service (DDoS) attack that briefly disrupted and slowed access to sites in the .cn domain.

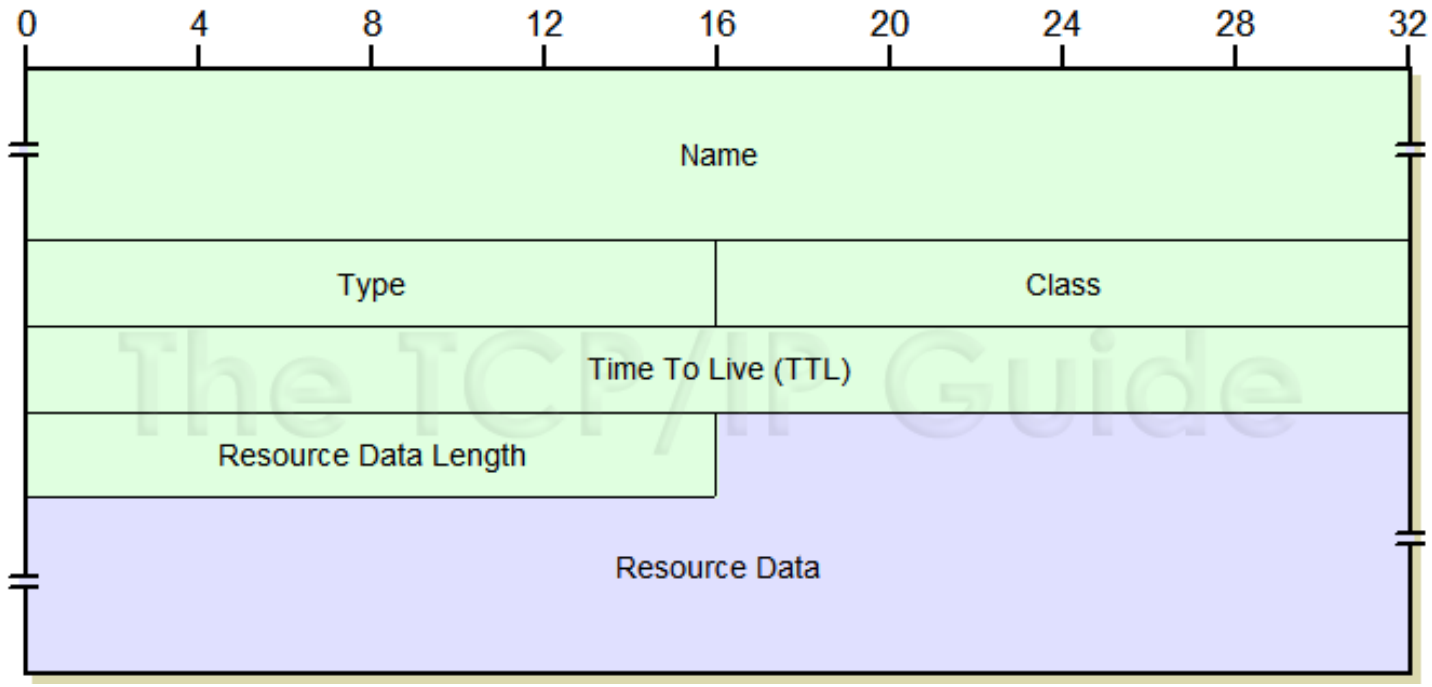
The DDoS attack was the largest in history against the domain servers for China's .cn ccTLD (country code top level domain), according to the China Internet Network Information Center (CNNIC), which administers the domain.

The first attack started Sunday around midnight Beijing time, and was then succeeded by a larger attack at 4 a.m, the CNNIC said in an Internet posting. A number of sites were affected, but Internet service to the sites had been gradually restored by 10 a.m. Sunday

It's unclear where the attack originated from or if it was still continuing. A CNNIC spokeswoman said on Monday it would update the public once more information was gathered. Chinese regulators have already launched unspecified measures to protect the domain system, while CNNIC has apologized for the disruption.

In DNS, data are stored as Resource Records (RRs).

All RRs have the same format as follows:



TTL: specifies the time interval in seconds that the RR can be cached at the client

Besides storing hostname-to-address mapping, DNS also stores other types of information:

The common types of RRs are:

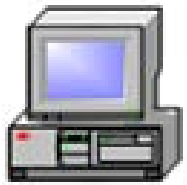
Type	*Mnemonic*	*Description*
1	A	**Address.** A 32-bit IPv4 address. It converts a domain name to an address.
2	NS	**Name server.** It identifies the authoritative servers for a zone.
5	CNAME	**Canonical name.** It defines an alias for the official name of a host.
15	MX	**Mail exchange.** It redirects mail to a mail server.
28	AAAA	**Address.** An IPv6 address.

The common class of RRs is:

Class	*Mnemonic*	*Description*
1	IN	Internet

Examples of RRs stored in different DNS. Here, we'll only focus on the important fields < name, type, value > :

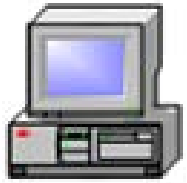
root server



a.root-servers.net

< sg., NS, dsany.sgnic.sg. >
< dsany.sgnic.sg., A, 194.0.1.16 >
< dsany.sgnic.sg., AAAA, 2001:678:4::10 >

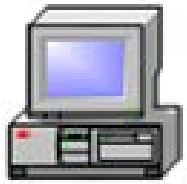
TLD server



dsany.sgnic.sg

< ntu.edu.sg., NS, dnstex.ntu.edu.sg. >
< dnstex.ntu.edu.sg., A, 155.69.254.5 >

authoritative server

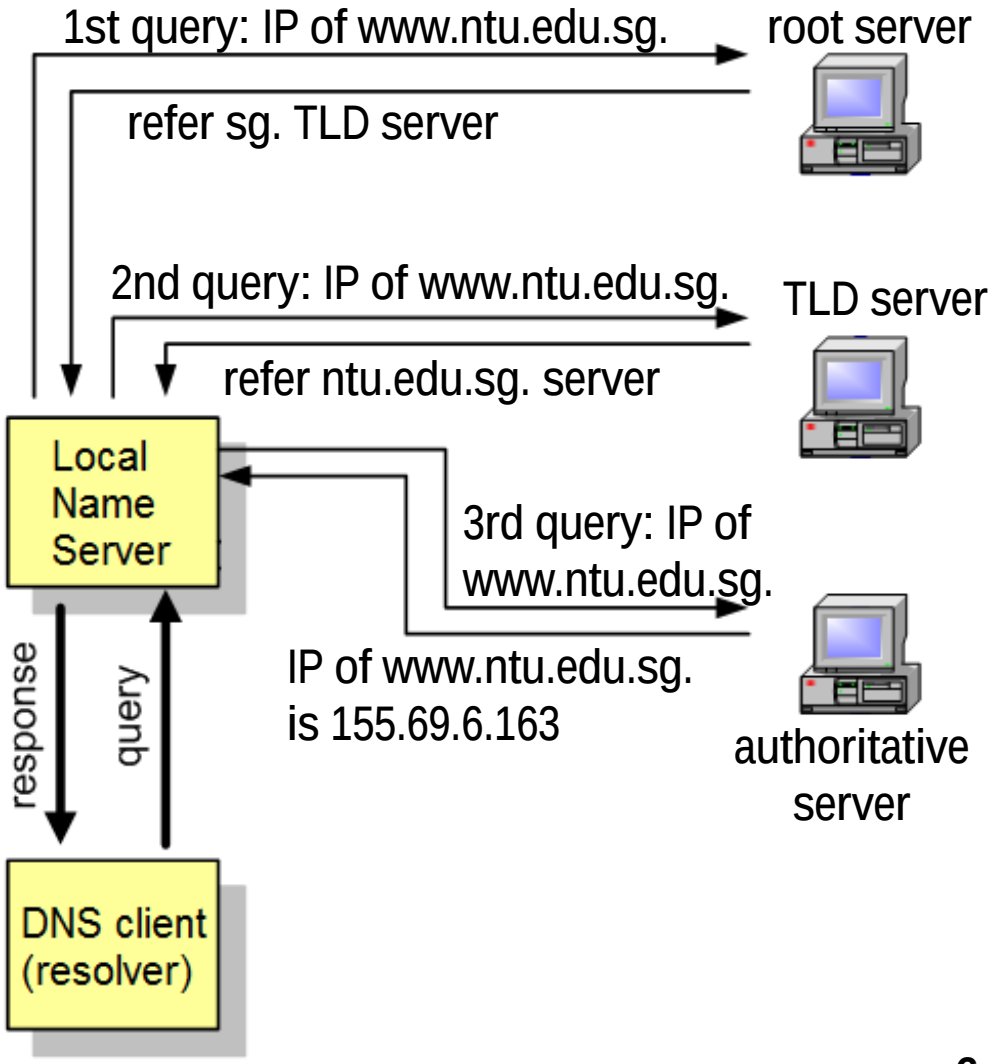


dnstex.ntu.edu.sg

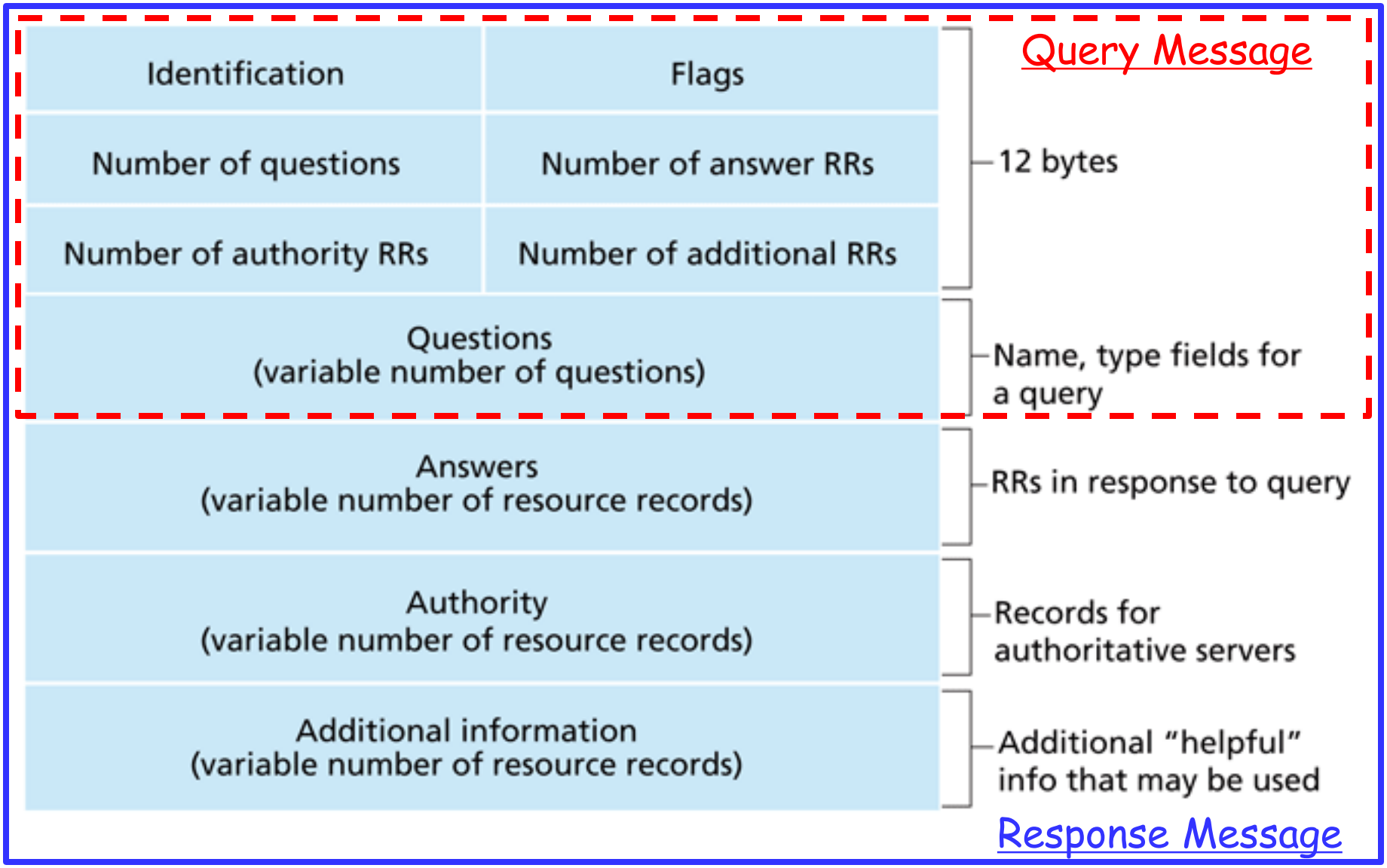
< www.ntu.edu.sg., A, 155.69.6.163 >
< ntu.edu.sg., MX, smtp.ntu.edu.sg. >
< smtp.ntu.edu.sg., A, 155.69.5.227 >

Name servers may be configured to support recursive or iterative queries. Typically, name resolution is done as follows:

- DNS client (resolver) contacts the local (default) name server.
- Local name server (usually recursive) will assist client to perform further queries if it does not know the answer.
- Root and TLD name servers (usually iterative) will only send a referral if they do not know the answer.



DNS Query/Response Message Format

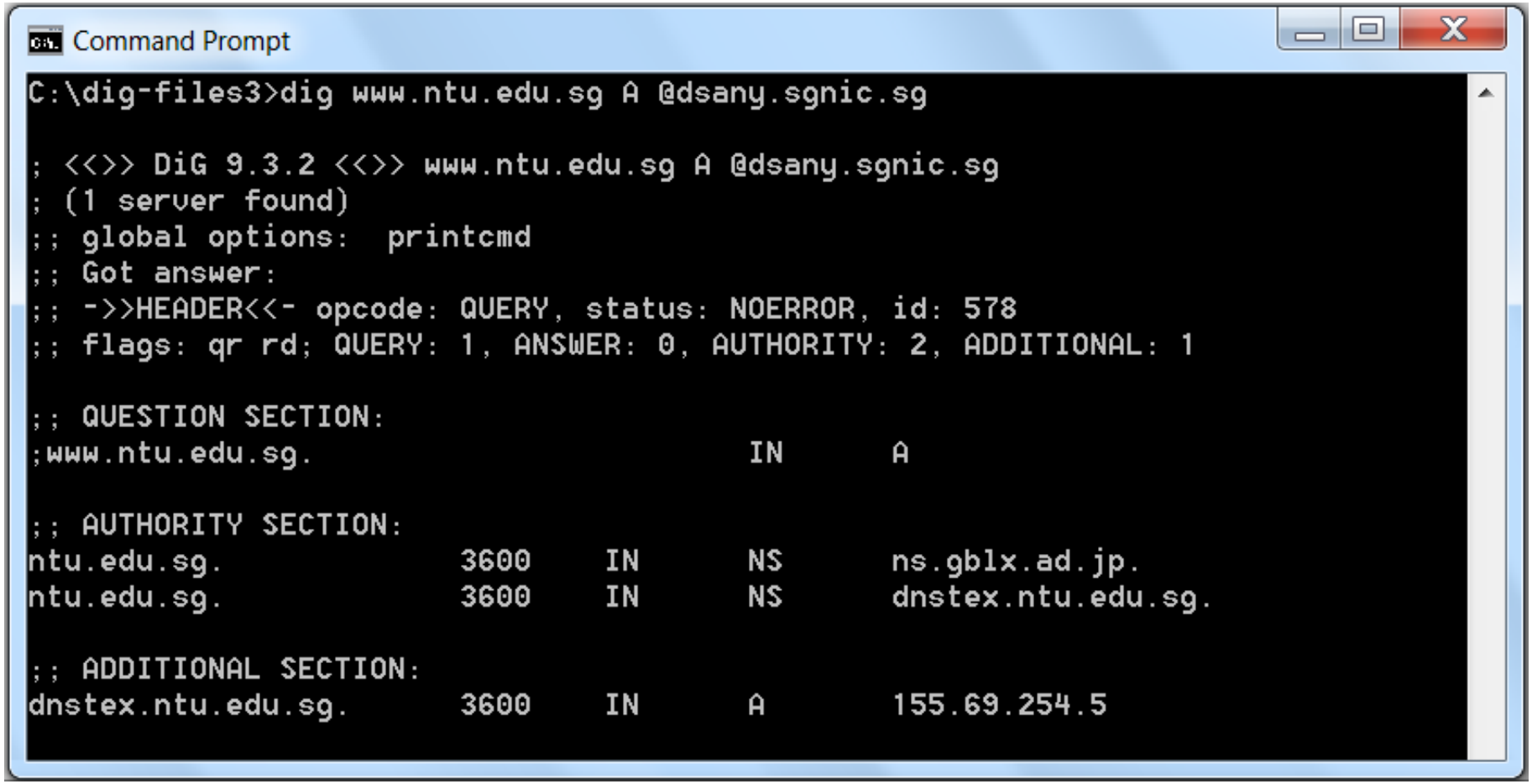


Example: using 'dig' command to query root server for IP of www.ntu.edu.sg:

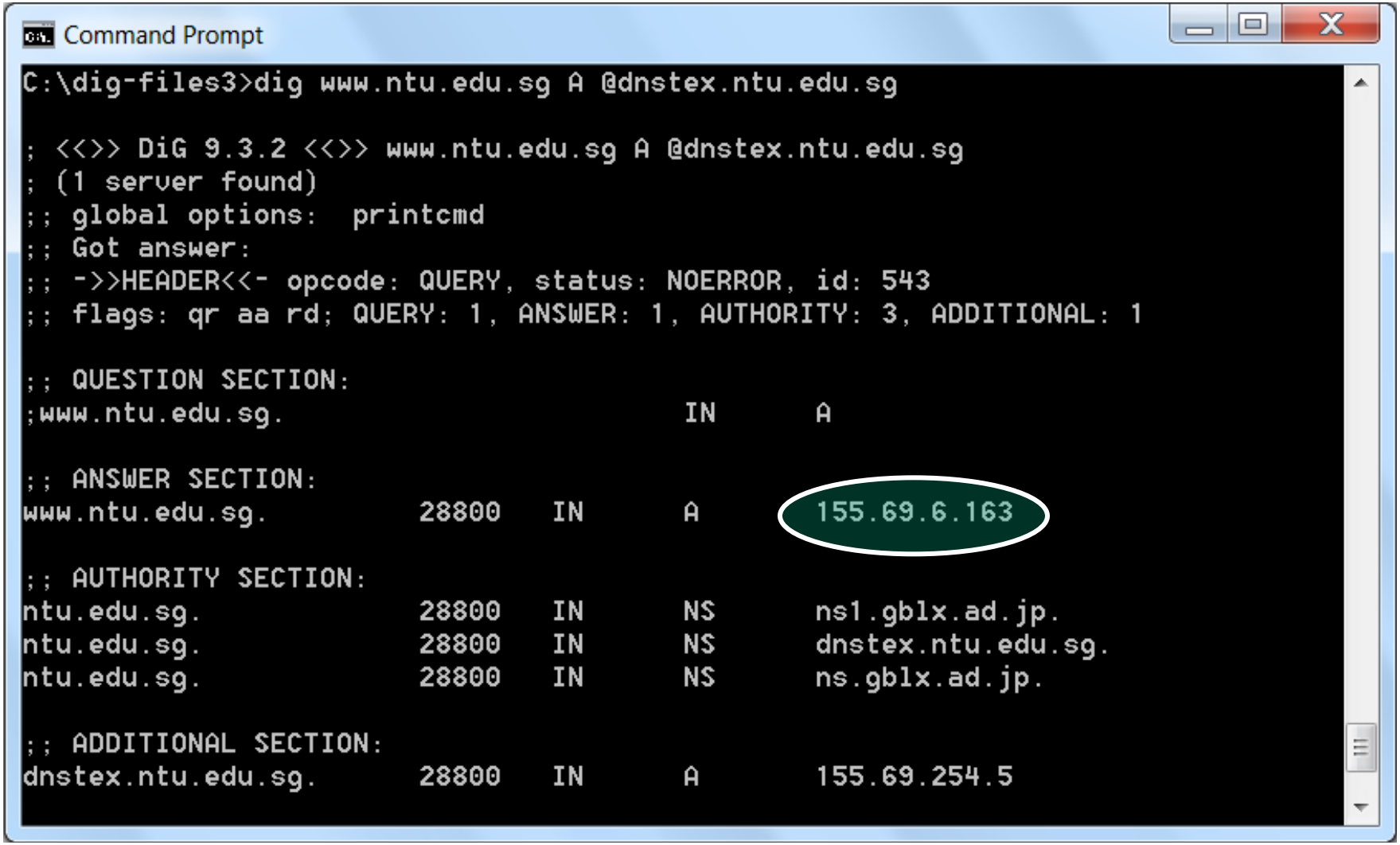
Command Prompt

```
C:\dig-files3>dig www.ntu.edu.sg A @a.root-servers.net

; <<>> DiG 9.3.2 <<>> www.ntu.edu.sg A @a.root-servers.net
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 480
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8

;; QUESTION SECTION:
;www.ntu.edu.sg.                        IN      A

;; AUTHORITY SECTION:
sg.                     172800  IN      NS      sec3.apnic.net.
sg.                     172800  IN      NS      ns2.cuhk.edu.hk.
sg.                     172800  IN      NS      sg-ns.anycast.pch.net.
sg.                     172800  IN      NS      dsany.sgnic.sg.

;; ADDITIONAL SECTION:
sec3.apnic.net.         172800  IN      AAAA    2001:dc0:1:0:4777::140
sec3.apnic.net.         172800  IN      A       202.12.28.140
ns2.cuhk.edu.hk.        172800  IN      AAAA    2405:3000:3:60::21
ns2.cuhk.edu.hk.        172800  IN      A       137.189.6.21
sg-ns.anycast.pch.net.  172800  IN      AAAA    2001:500:14:6057:ad::1
sg-ns.anycast.pch.net.  172800  IN      A       204.61.216.57
dsany.sgnic.sg.         172800  IN      AAAA    2001:678:4::10
dsany.sgnic.sg.         172800  IN      A       194.0.1.16
```

Example: using 'dig' command to query TLD server dsany.sgnic.sg for IP of www.ntu.edu.sg:

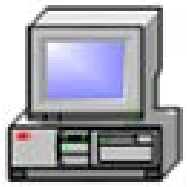


Example: using 'dig' command to query authoritative server dnstex.ntu.edu.sg for IP of www.ntu.edu.sg:



Examples of RRs stored in different DNS. Here, we'll only focus on the important fields < name, type, value > :

root server

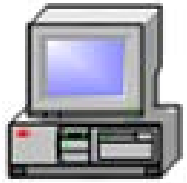


a.root-servers.net

< sg., NS, dsany.sgnic.sg. >
< dsany.sgnic.sg., A, 194.0.1.16 >
< dsany.sgnic.sg., AAAA, 2001:678:4::10 >

194.0.1.16

TLD server

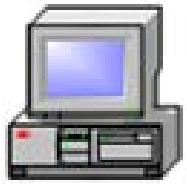


dsany.sgnic.sg

< ntu.edu.sg., NS, dnstex.ntu.edu.sg. >
< dnstex.ntu.edu.sg., A, 155.69.254.5 >

authoritative server

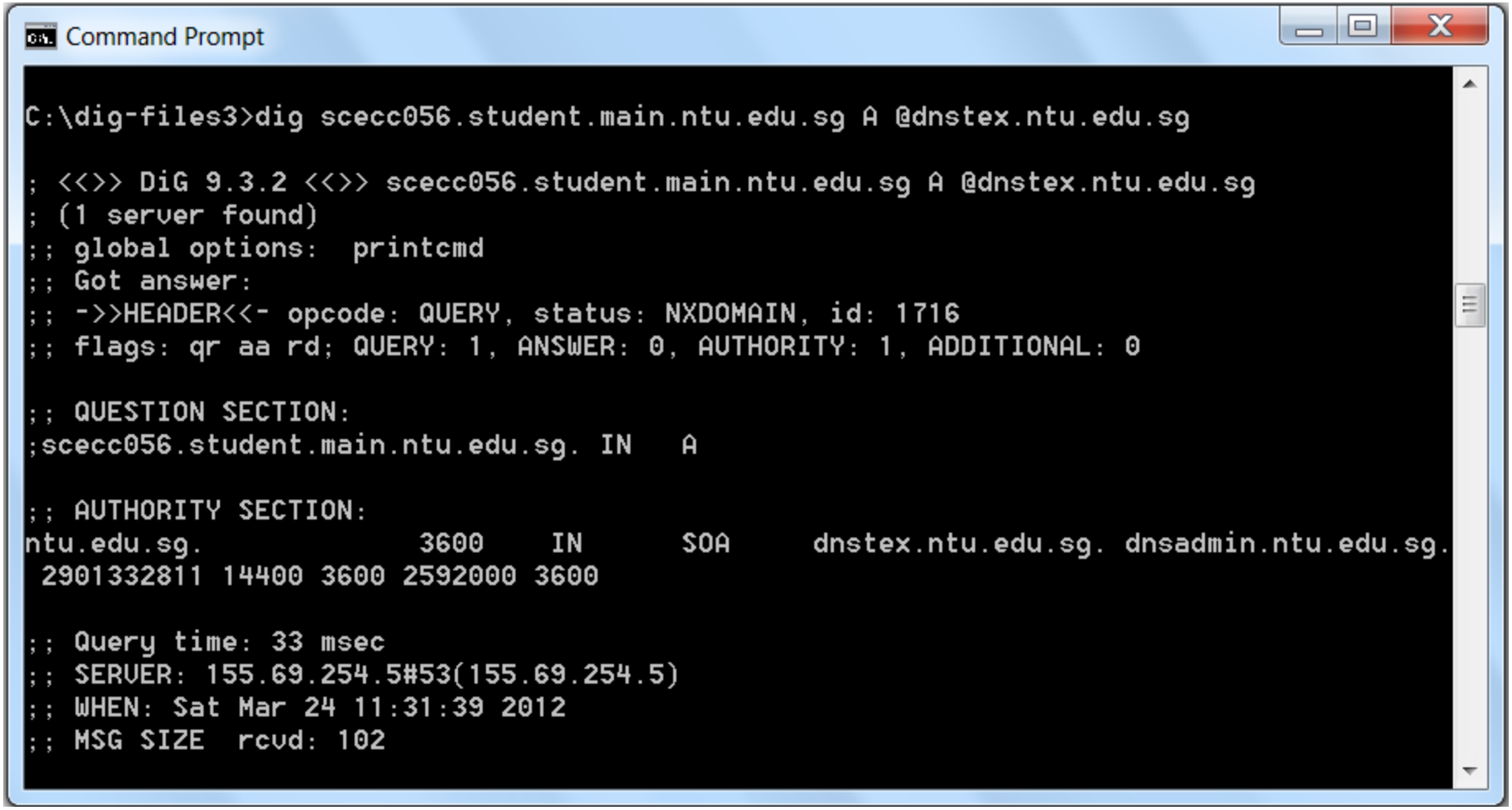
155.69.254.5



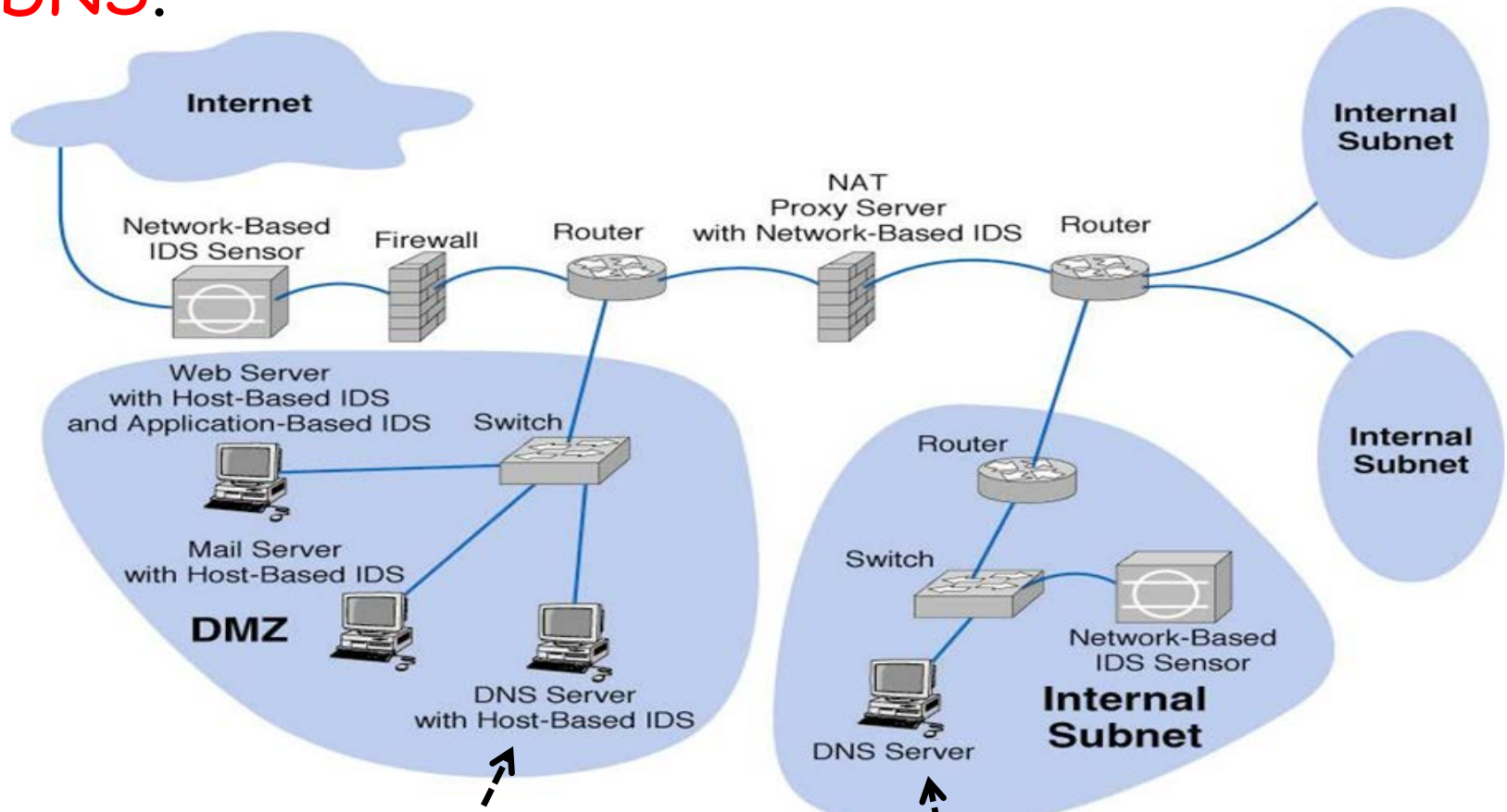
dnstex.ntu.edu.sg

< www.ntu.edu.sg., A, 155.69.6.163 >
< ntu.edu.sg., MX, smtp.ntu.edu.sg. >
< smtp.ntu.edu.sg., A, 155.69.5.227 >

However, querying authoritative server dnstex.ntu.du.sg did not return IP for scecc056.student.main.ntu.edu.sg. Why?



Note that for security purpose, organizations may implement separate external and internal DNS.



External DNS server in NTU:
dnstex.ntu.edu.sg
(155.69.254.5)

Internal DNS servers in NTU:
155.69.5.225, 155.69.5.7

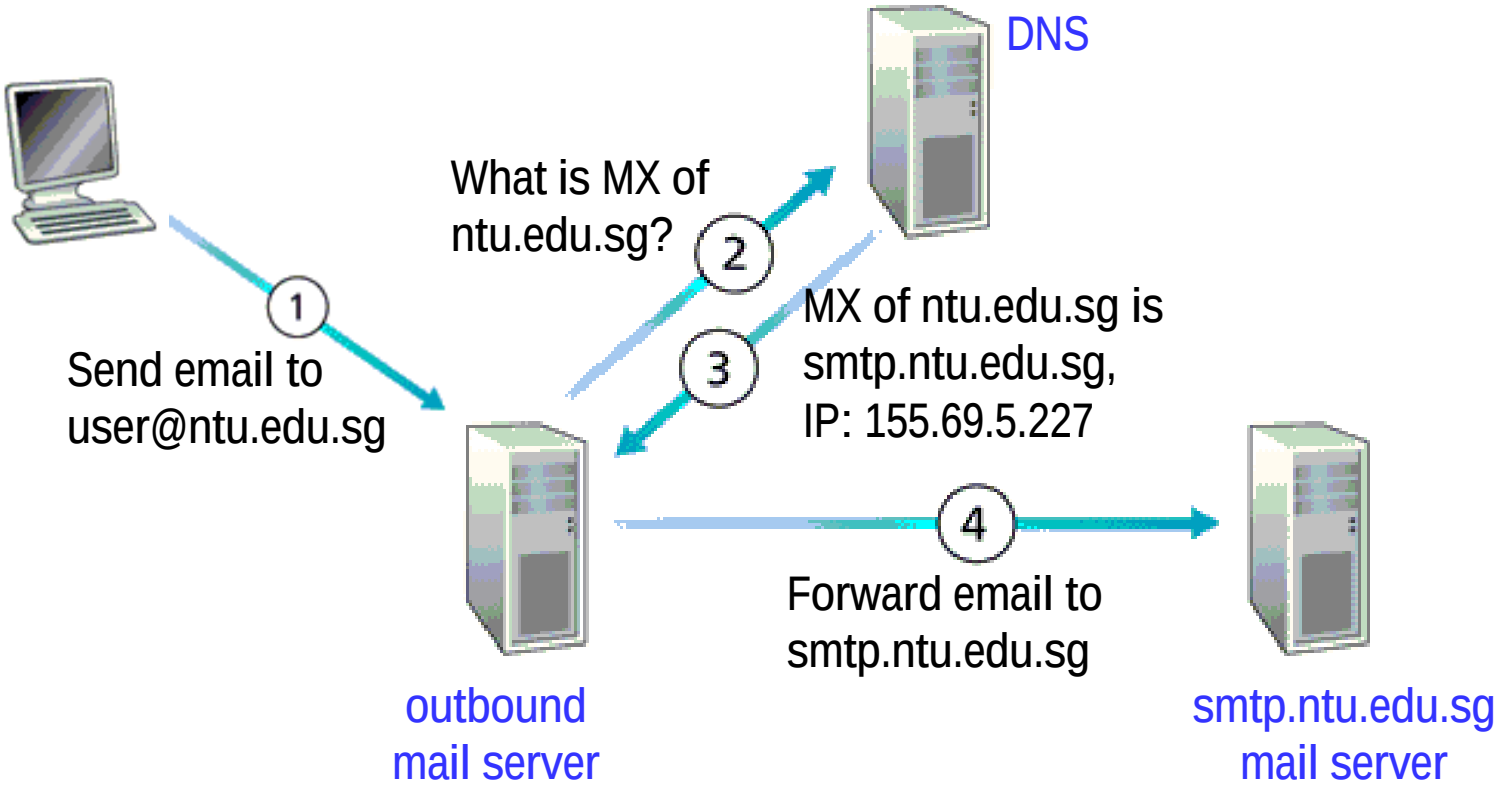
Querying internal DNS server:

```
C:\dig-files3>dig scecc056.student.main.ntu.edu.sg A @155.69.5.225

; <<>> DiG 9.3.2 <<>> scecc056.student.main.ntu.edu.sg A @155.69.5.225
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1447
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;scecc056.student.main.ntu.edu.sg. IN   A

;; ANSWER SECTION:
scecc056.student.main.ntu.edu.sg. 1079 IN A     155.69.142.89

;; AUTHORITY SECTION:
student.main.ntu.edu.sg. 2964   IN      NS      student10.student.main.ntu.edu.sg.
student.main.ntu.edu.sg. 2964   IN      NS      student11.student.main.ntu.edu.sg.
student.main.ntu.edu.sg. 2964   IN      NS      student20.student.main.ntu.edu.sg.

;; ADDITIONAL SECTION:
student10.student.main.ntu.edu.sg. 60 IN A      155.69.5.153
student11.student.main.ntu.edu.sg. 1869 IN A    155.69.5.155
student20.student.main.ntu.edu.sg. 58 IN A      155.69.4.84

;; Query time: 31 msec
;; SERVER: 155.69.5.225#53(155.69.5.225)
;; WHEN: Fri Mar 23 16:50:40 2012
;; MSG SIZE  rcvd: 186
```

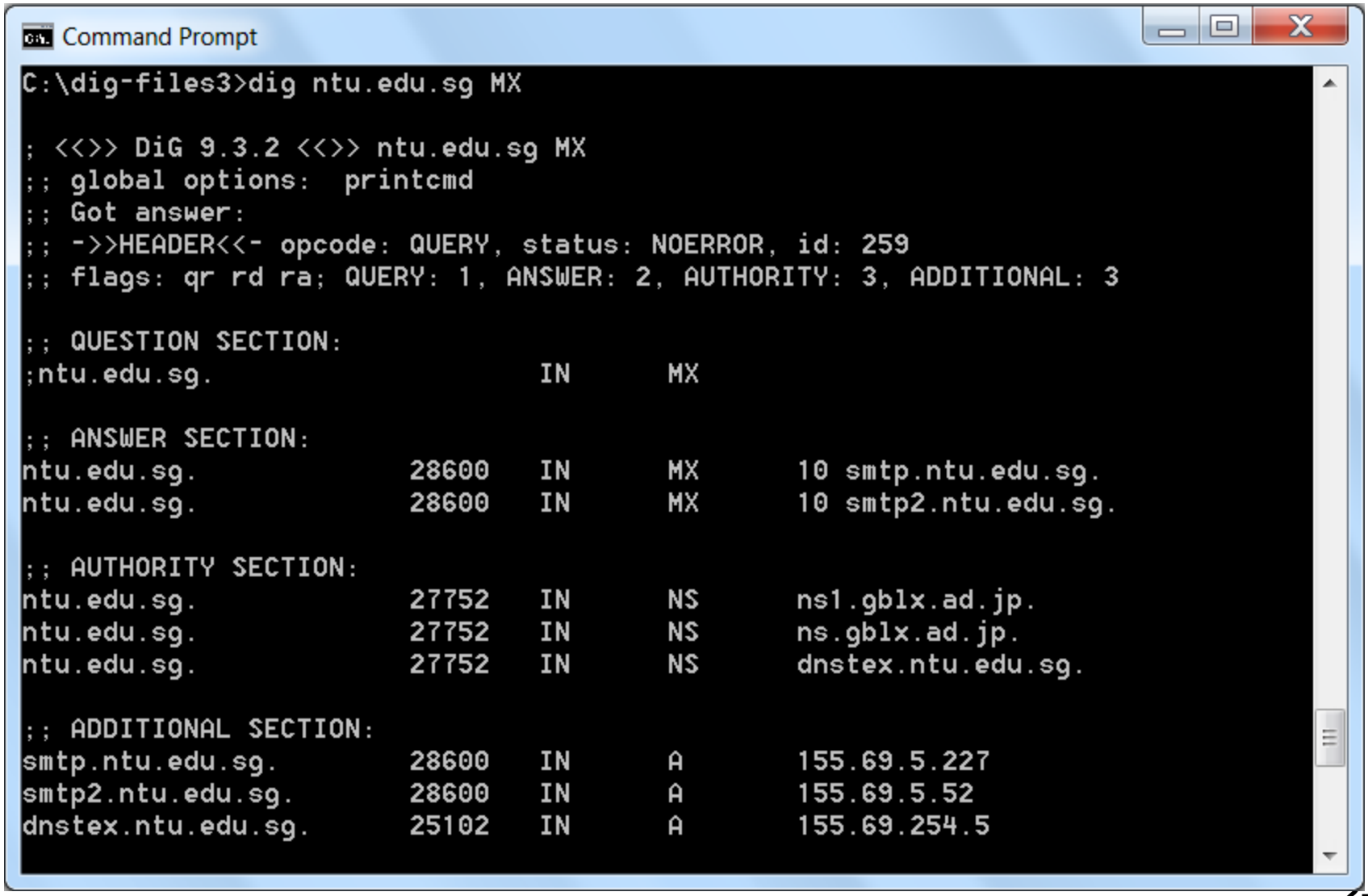
Besides resolving domain name to IP address, DNS also enables email address to look simply by using MX RR to resolve mail servers.

For example:

user@ntu.edu.sg instead of user@smtp.ntu.edu.sg

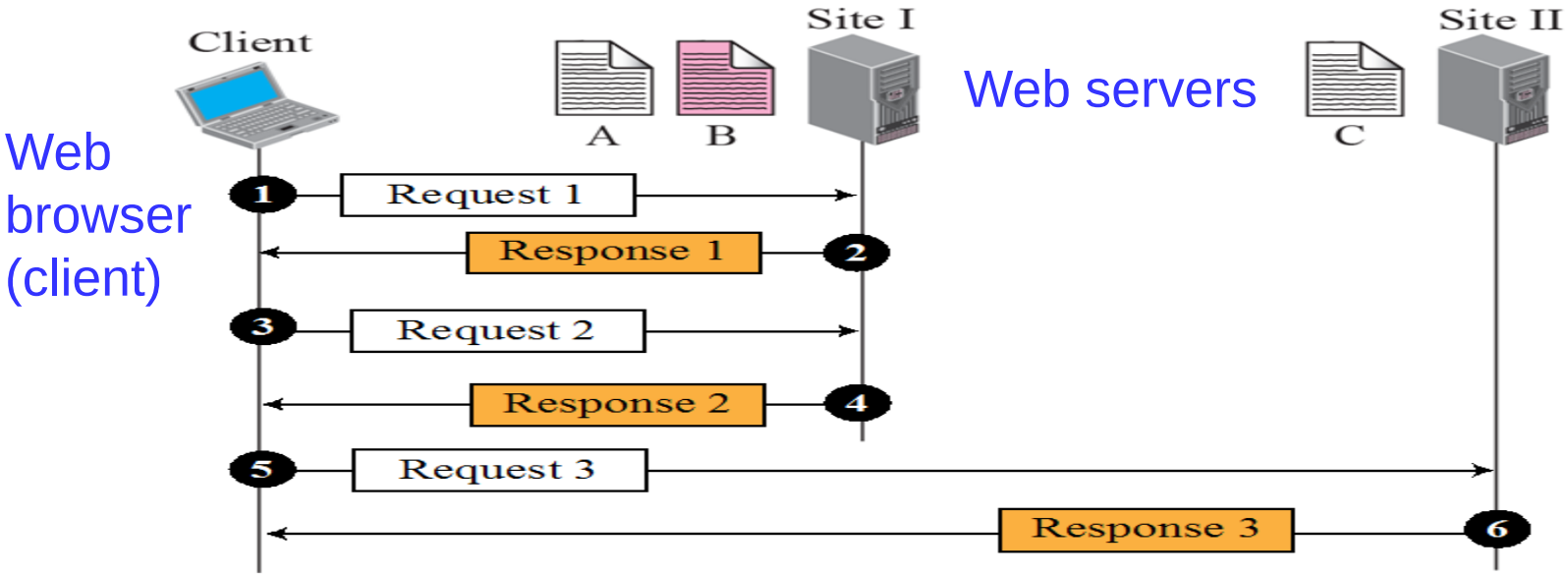


Example: using 'dig' command to query authoritative server dnstex.ntu.edu.sg server for MX of ntu.edu.sg:



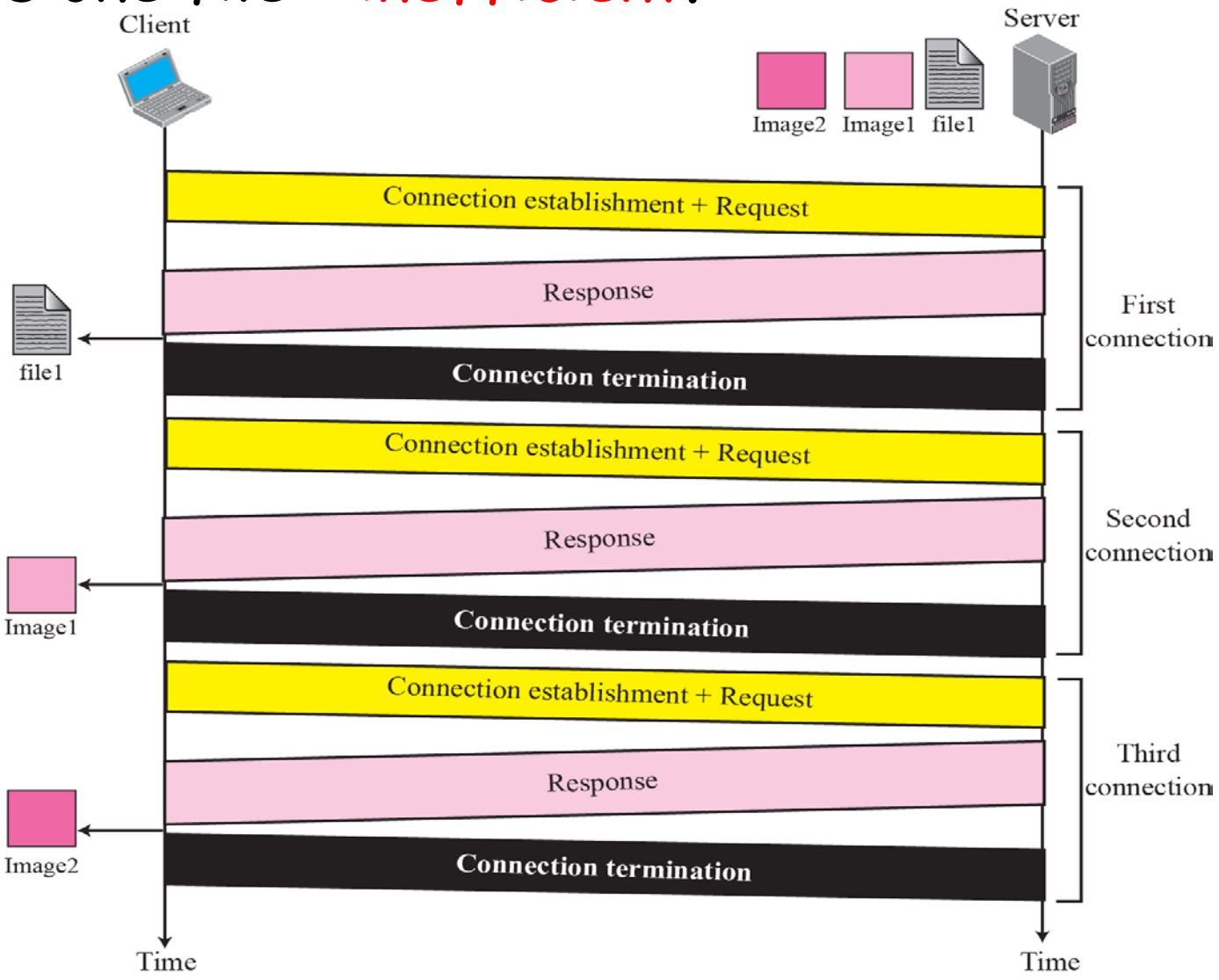
WWW and HTTP

- World Wide Web (WWW) is simply a network application which allows a client to access a file from a server.

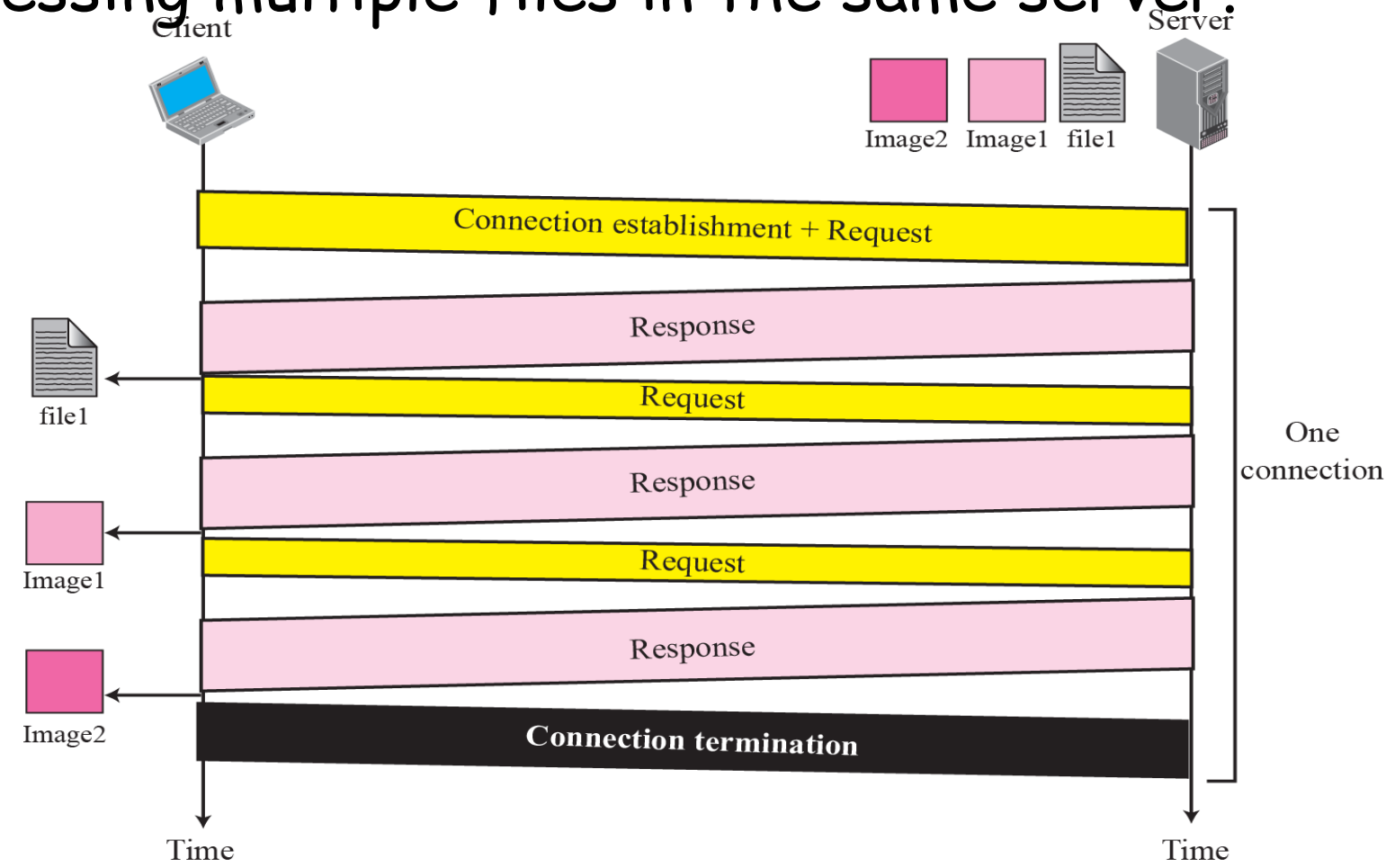


- HyperText Transfer Protocol (HTTP) is the application layer protocol used by WWW. It is designed to run over TCP with server listening at well-known port 80.
- Basically, HTTP consists of request/response messages.

Non-persistent HTTP: individual TCP connection/ termination for each pair of request/response to access one file – inefficient.



Persistent HTTP: multiple request/response messages within one TCP connection – efficient for accessing multiple files in the same server.



Persistent HTTP is the default mode for HTTP 1.1 whereas HTTP 1.0 needs to use header field "Connection: Keep-Alive".

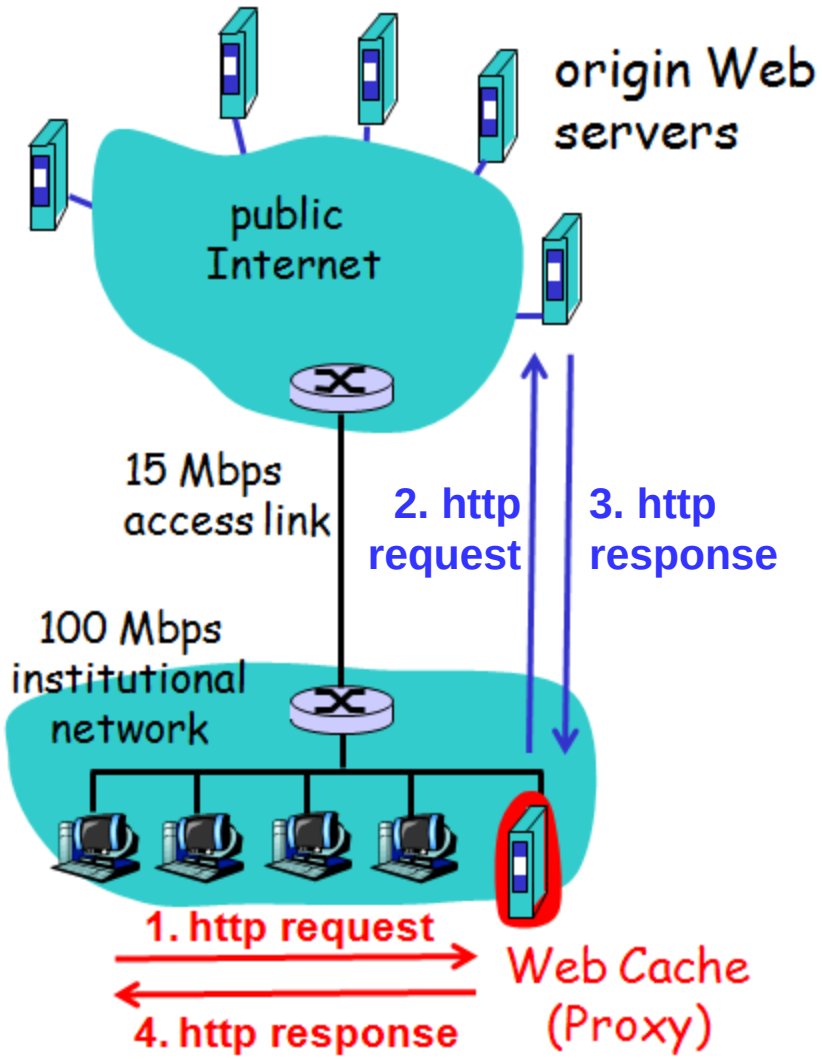
Web Proxy (Cache)

Why Web Proxy?

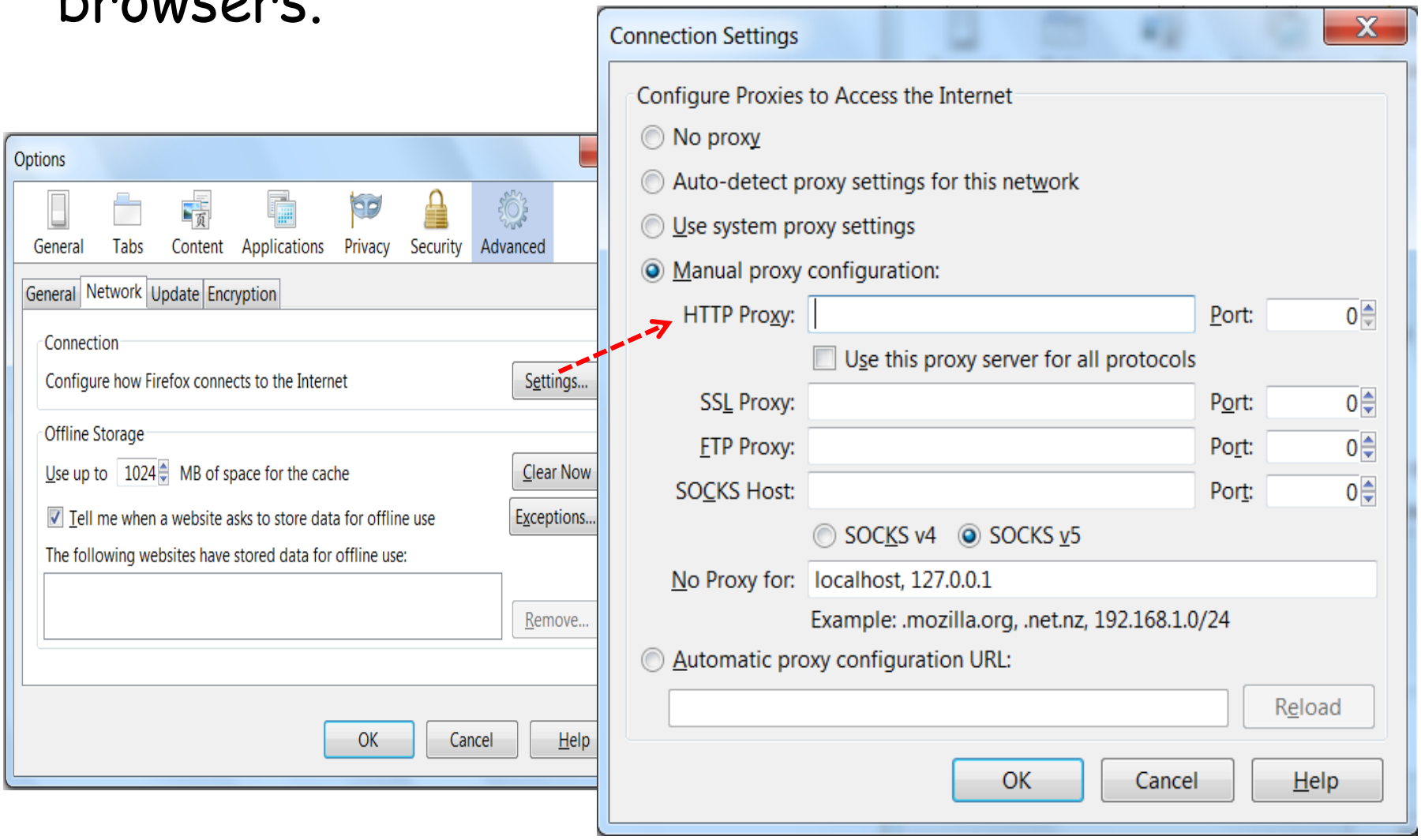
- Improve performance by caching
- Reduce traffic load on costly access link
- Monitor/Filter contents

How Web Proxy Works?

1. Client requests to proxy
2. (if content not available) proxy requests to origin server
3. Origin server responds to proxy
4. Proxy responds to client

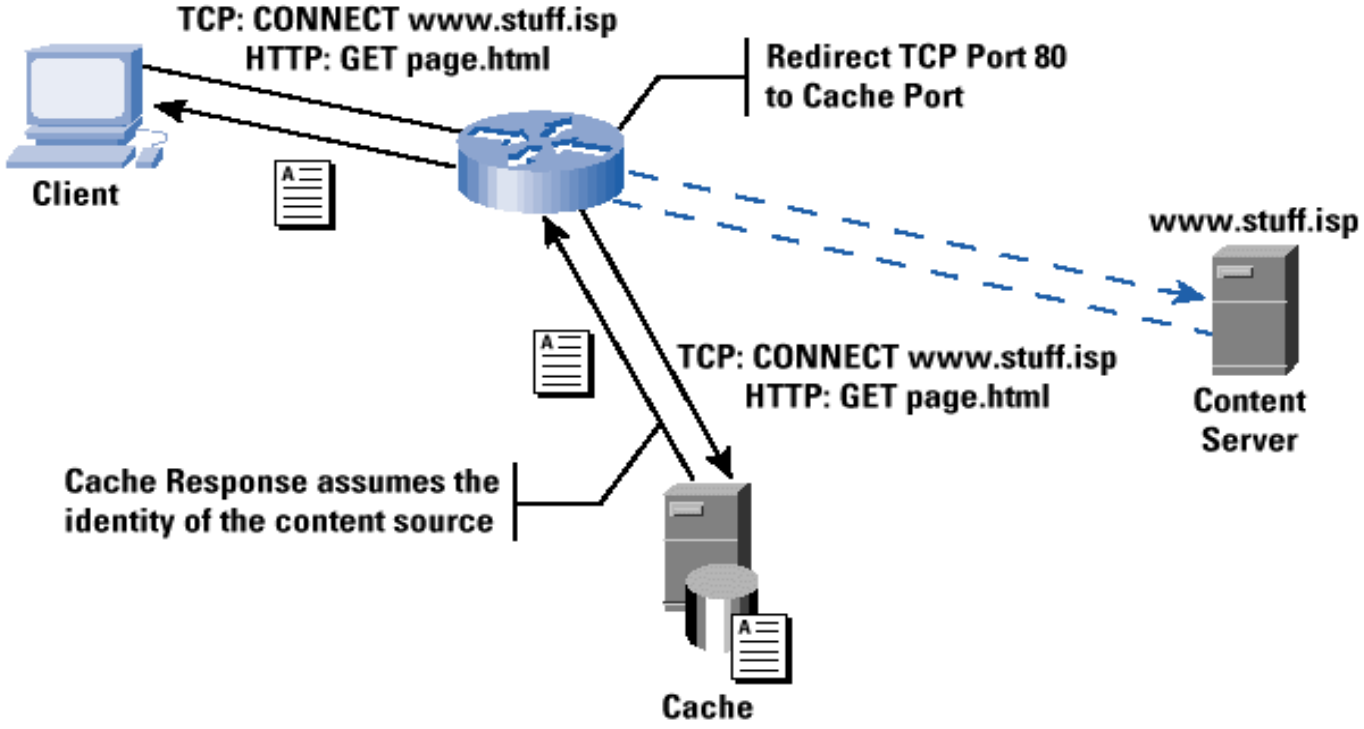


Traditionally, Web proxy is implemented by requiring users to explicitly configure their browsers.

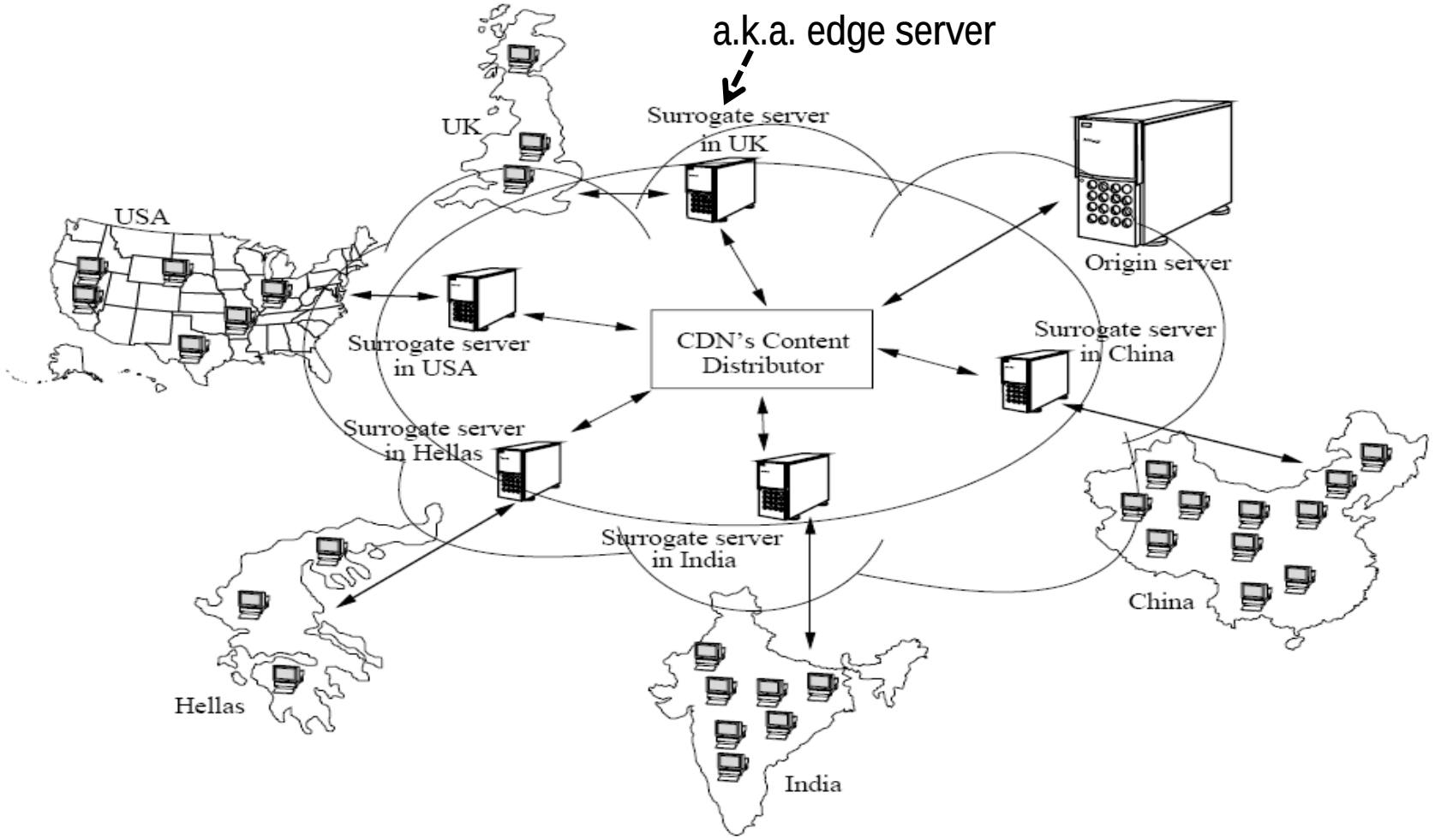


However, note that Web proxy can be implemented transparently without the knowledge of users/servers!

Basically, the organization/ISP configures its routers to intercept all Web traffic and re-direct (mis-direct) them to its Web proxy, which masquerades as the destination server!



Alternatively, if performance is important, an option for content provider is to use the service of Content Delivery/ Distribution Network (CDN).



For example, one of the world's largest CDN is Akamai network.

The Akamai CDN (2011):

85,000+ Servers	950+ Networks	660+ Cities	70+ Countries

Resulting in traffic of:

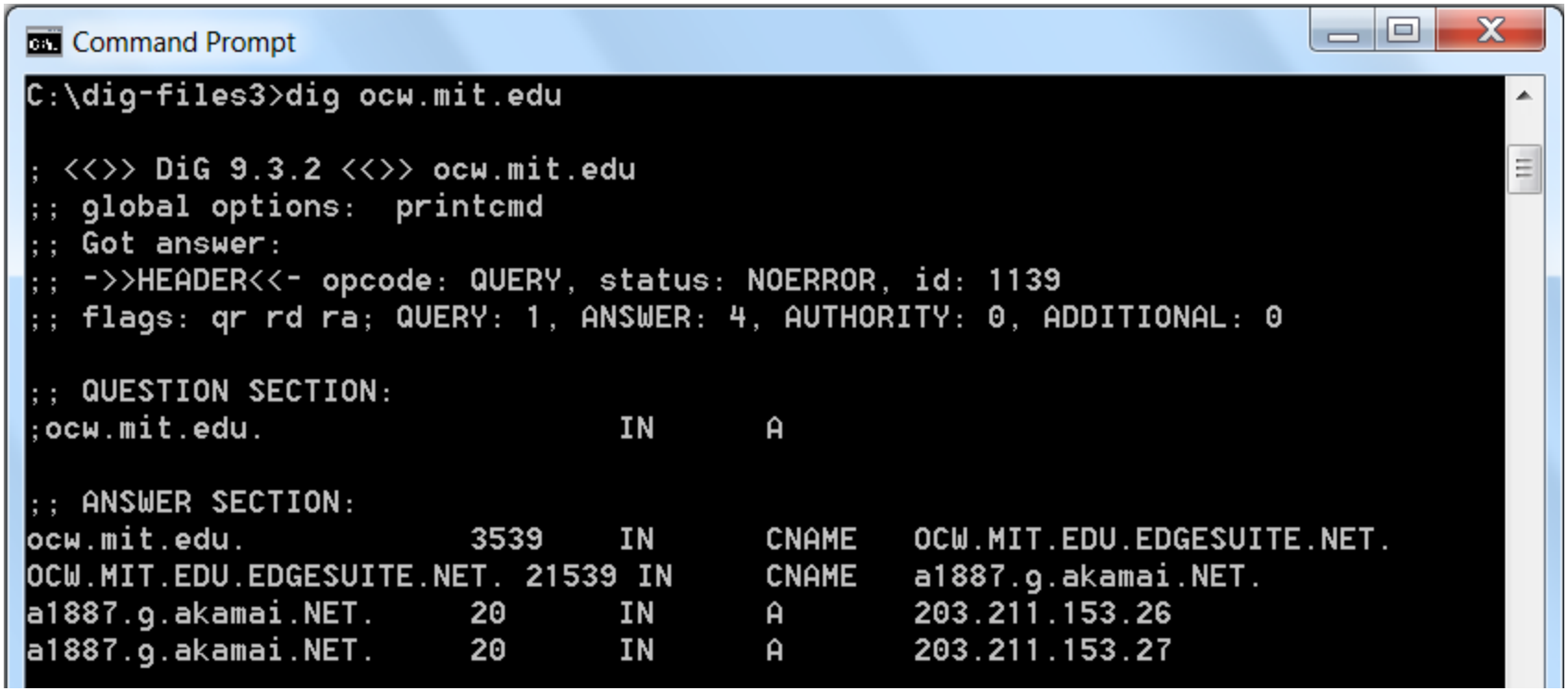
5.4 petabytes / day

790+ billion hits / day

436+ million unique clients IPs / day

With CDN, a Web request will be transparently re-directed, commonly implemented using DNS re-direction with CNAME RRs.

Eg.: MIT Open Course Ware site @http://ocw.mit.edu is using CDN service. If we access it from Singapore, we are re-directed to Akamai servers in Singapore.



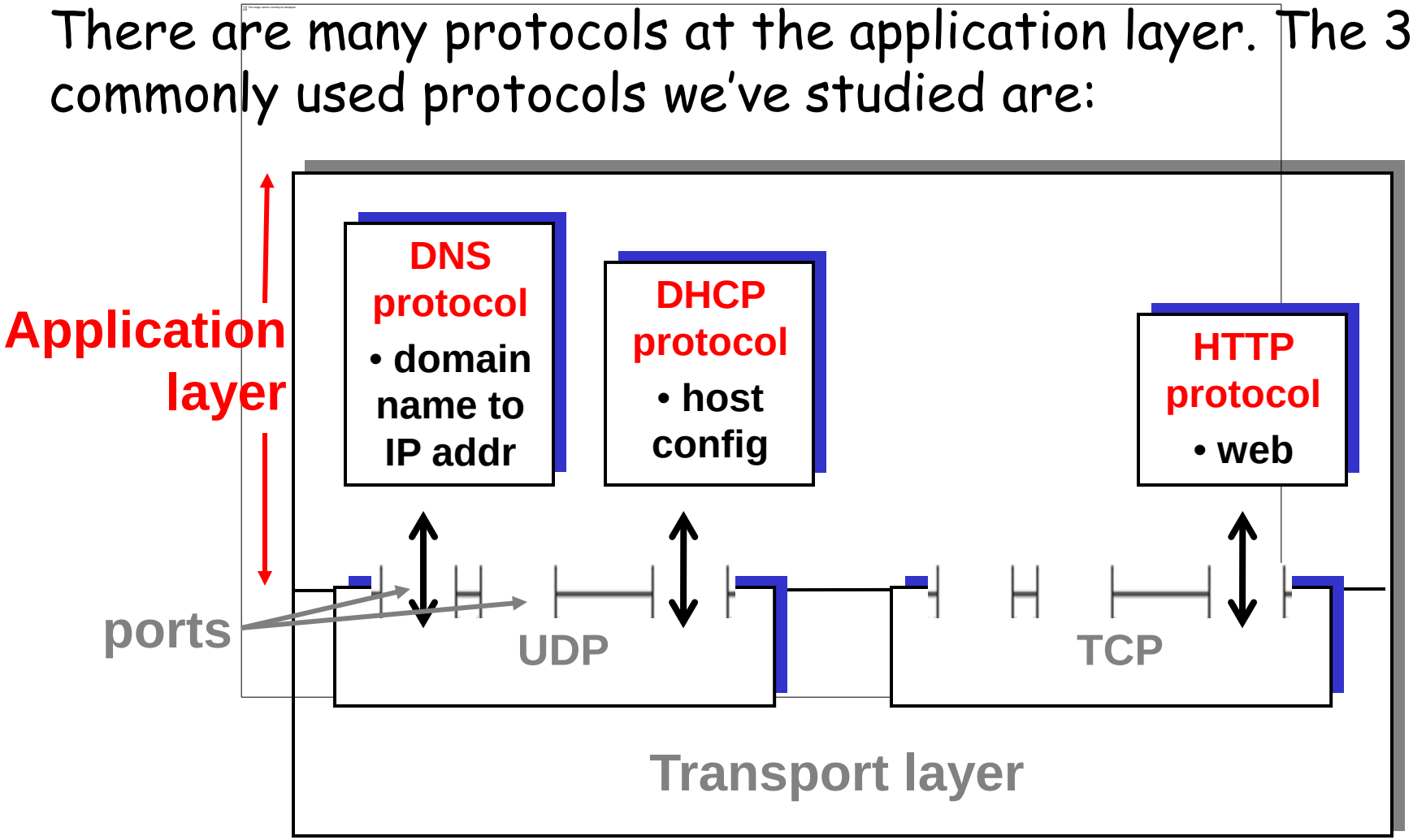
CDN and DNS re-direction with CNAME RRs:

However, if we were to access http://ocw.mit.edu from U.K. (e.g. 146.185.23.179), we would be re-directed to other Akamai servers.

```
; <<>> DiG 9.3.2 <<>> @ns.kloth.net ocw.mit.edu A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10791
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ocw.mit.edu.                   IN      A

;; ANSWER SECTION:
ocw.mit.edu.            106     IN      CNAME   OCW.MIT.EDU.EDGESUITE.NET.
OCW.MIT.EDU.EDGESUITE.NET. 18169 IN     CNAME   a1887.g.akamai.NET.
a1887.g.akamai.NET.     20      IN      A       92.123.68.64
a1887.g.akamai.NET.     20      IN      A       92.123.68.66

;; Query time: 5 msec
;; SERVER: 88.198.39.133#53(88.198.39.133)
;; WHEN: Sat Mar 24 10:57:27 2012
;; MSG SIZE  rcvd: 129
```

Summary of Application Layer

There are many protocols at the application layer. The 3 commonly used protocols we've studied are:



Finally, a review of what we have covered for Part I and II of the course: