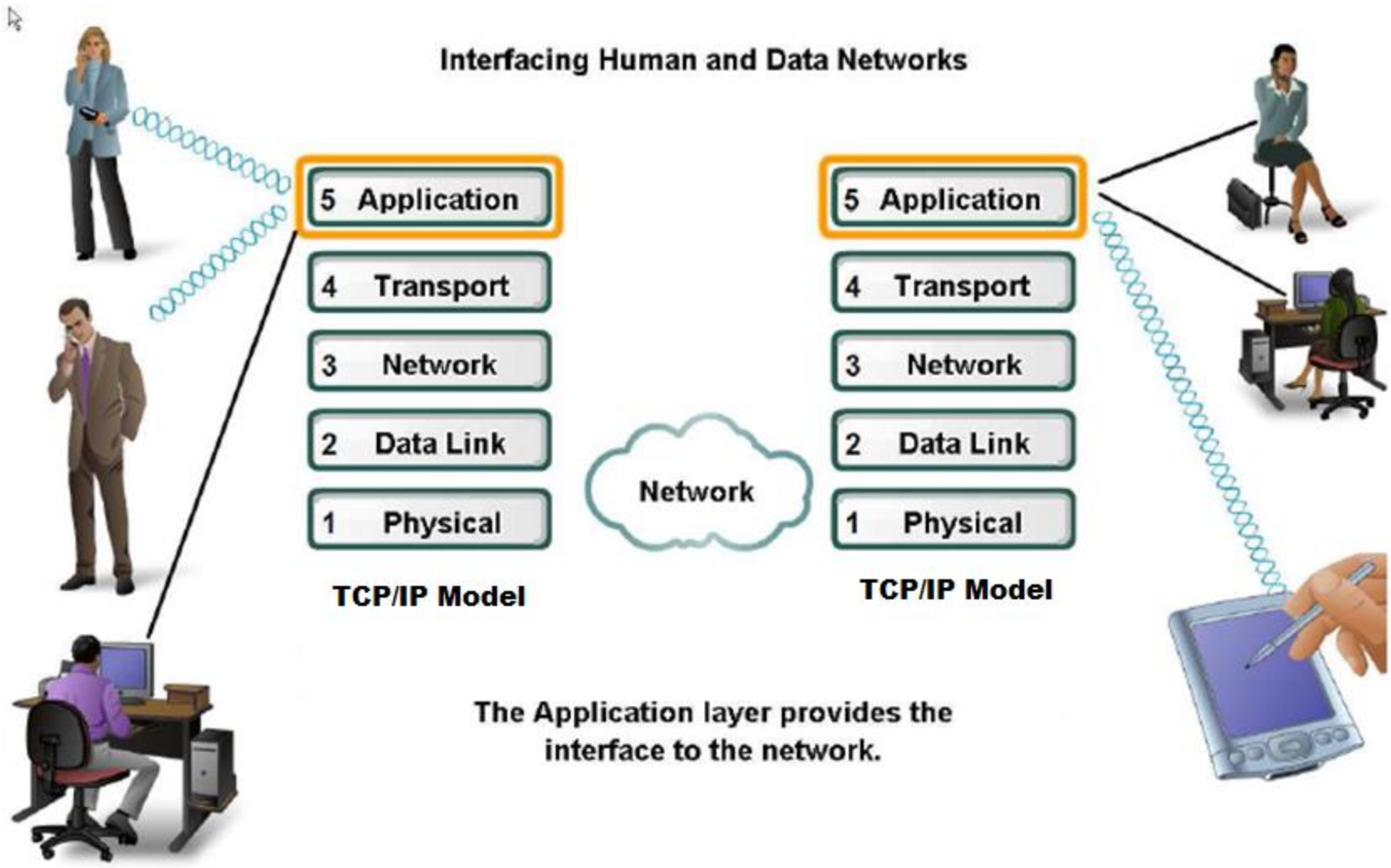
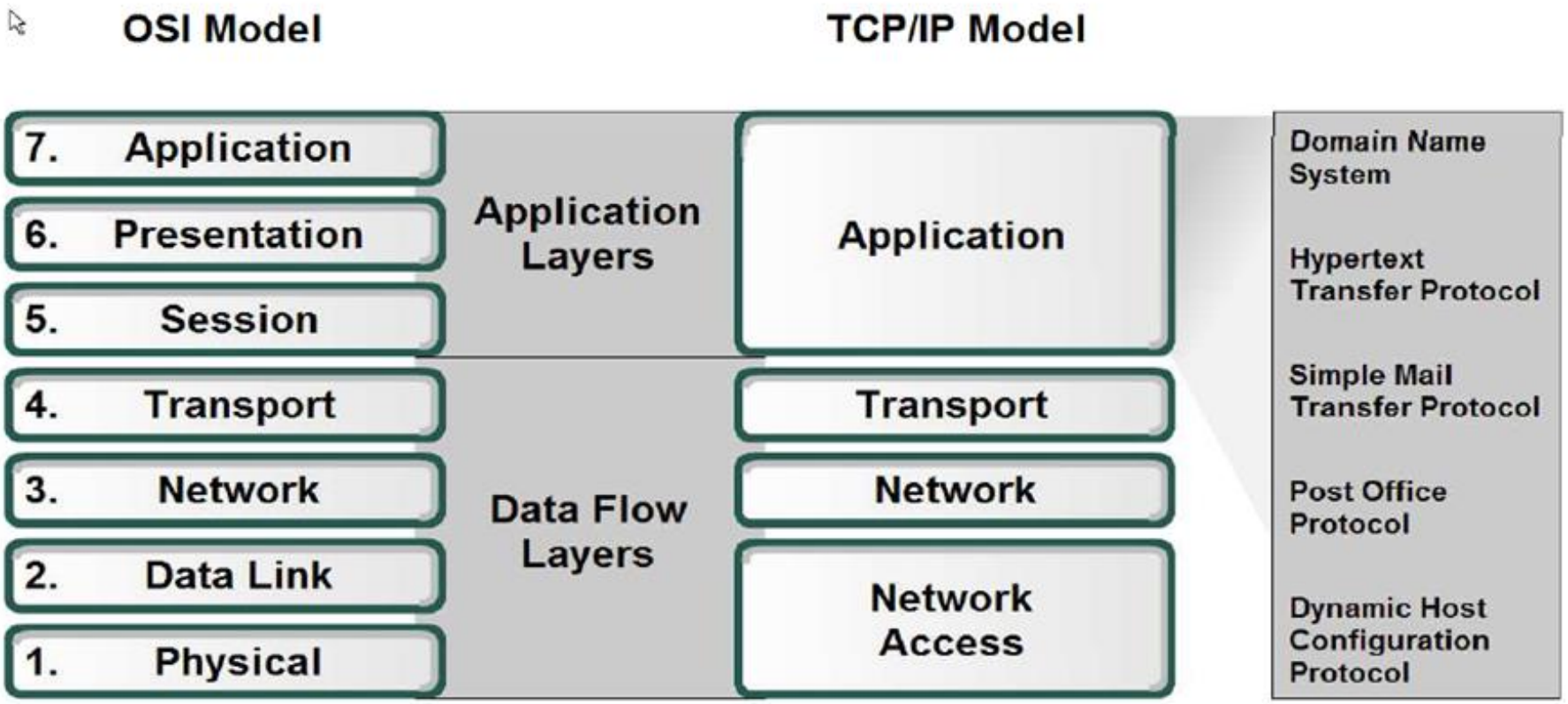
Application layer

Computer Networks

Faculty of Information Technology
Hanoi University

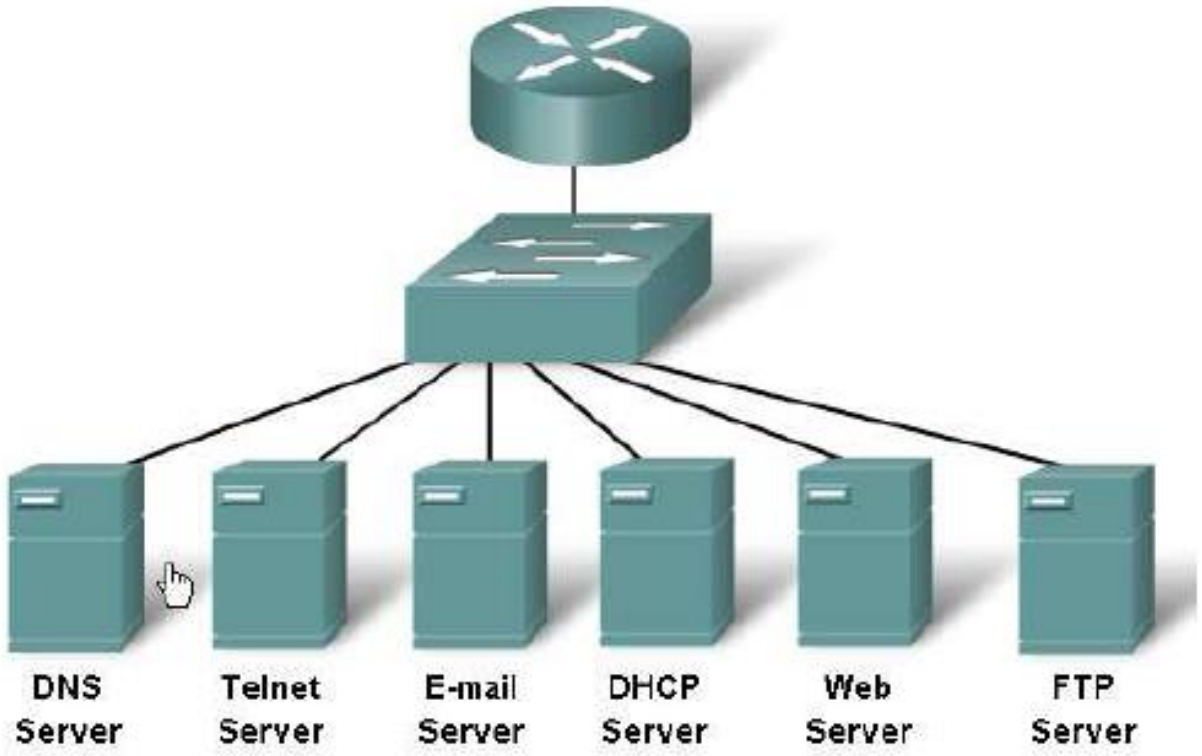

Interfacing Human and Data Networks
5 Application
4 Transport
3 Network
2 Data Link
1 Physical
TCP/IP Model
Network
5 Application
4 Transport
3 Network
2 Data Link
1 Physical
TCP/IP Model
The Application layer provides the interface to the network.

Application layer



Application layer

- DNS
- HTTP
- SMTP
- Telnet
- FTP
- DHCP
- SNMP
- …



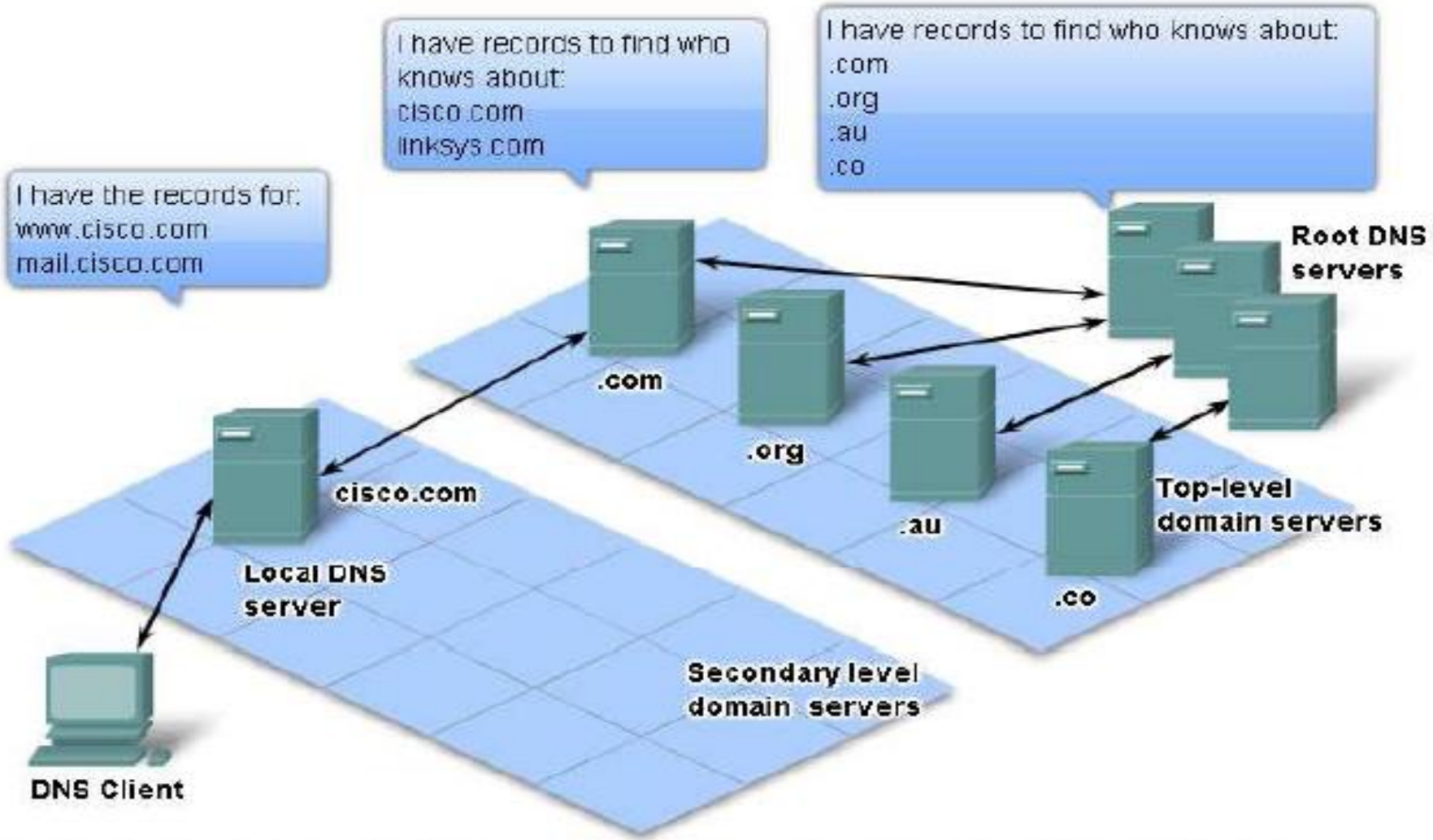
Port Number	Transport Protocol	Service Name	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

DNS

DNS

- The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
- A Domain Name Service translates queries for domain **names** (which are meaningful to humans) into **IP addresses** for the purpose of locating computer services and devices worldwide.

DNS

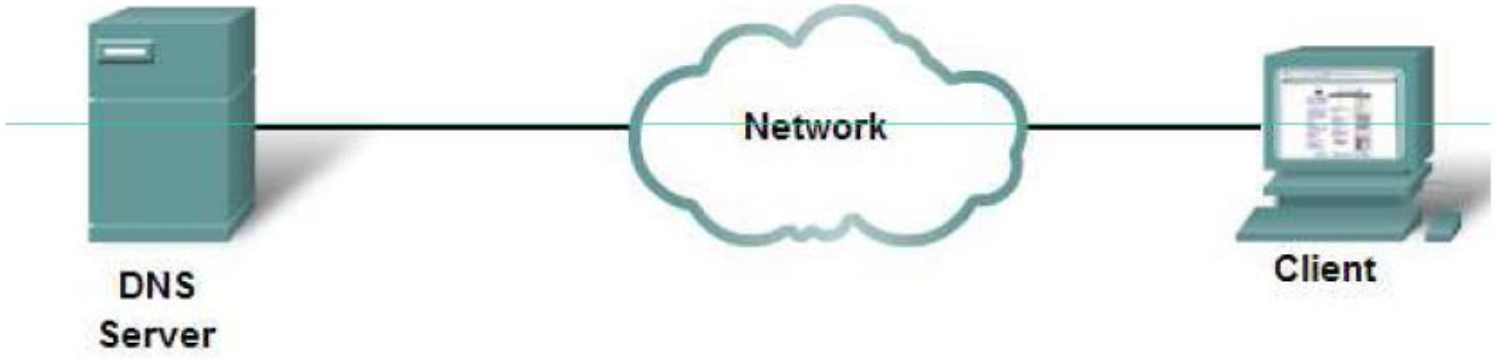


A hierarchy of DNS servers contains the resource records that match names with addresses.

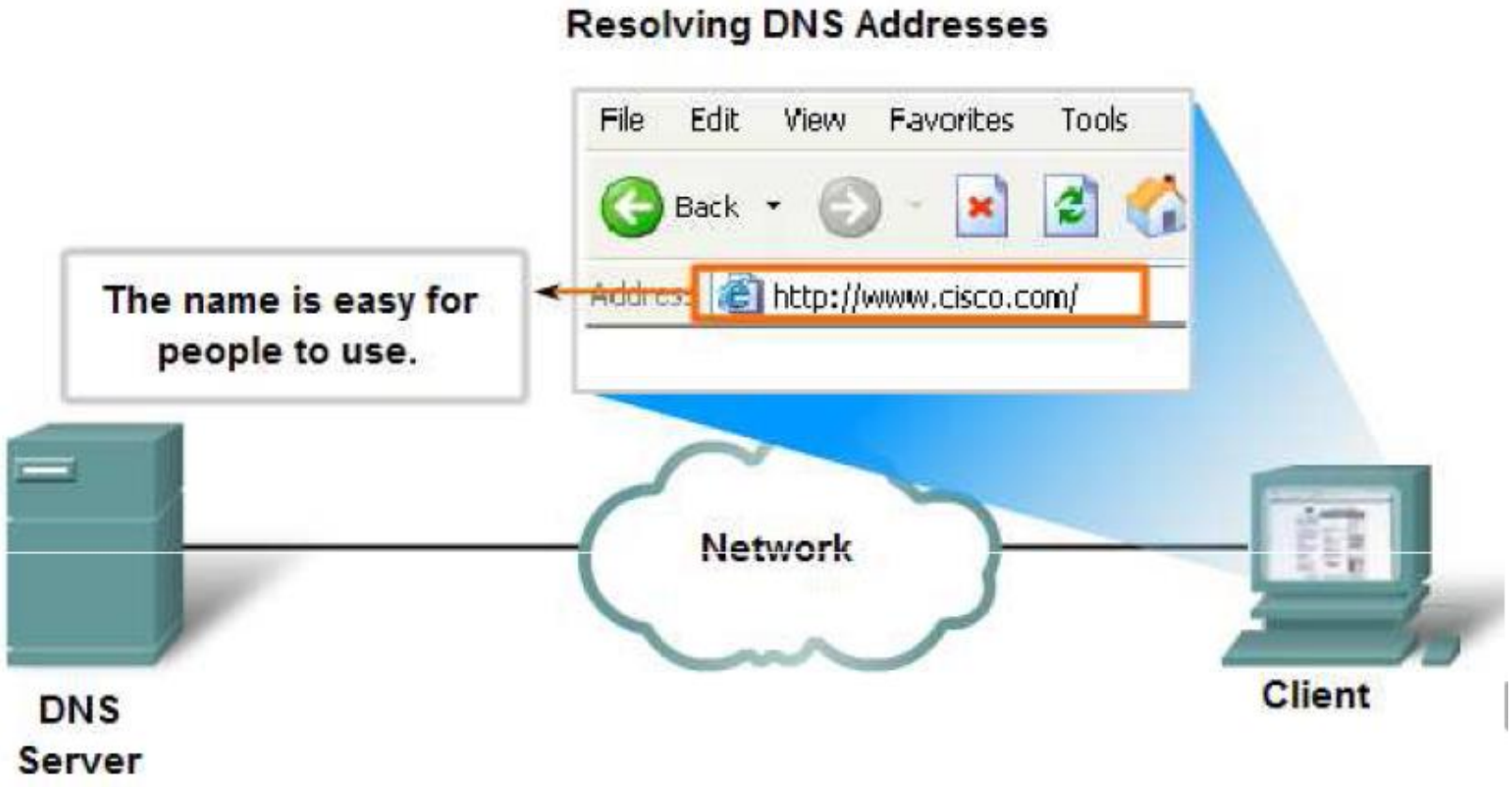
DNS

- DNS primarily uses User Datagram Protocol (UDP) on port number 53 to serve requests.
  - DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.
  - The Transmission Control Protocol (TCP) is used when the response data size exceeds 512 bytes, or for tasks such as zone transfers.

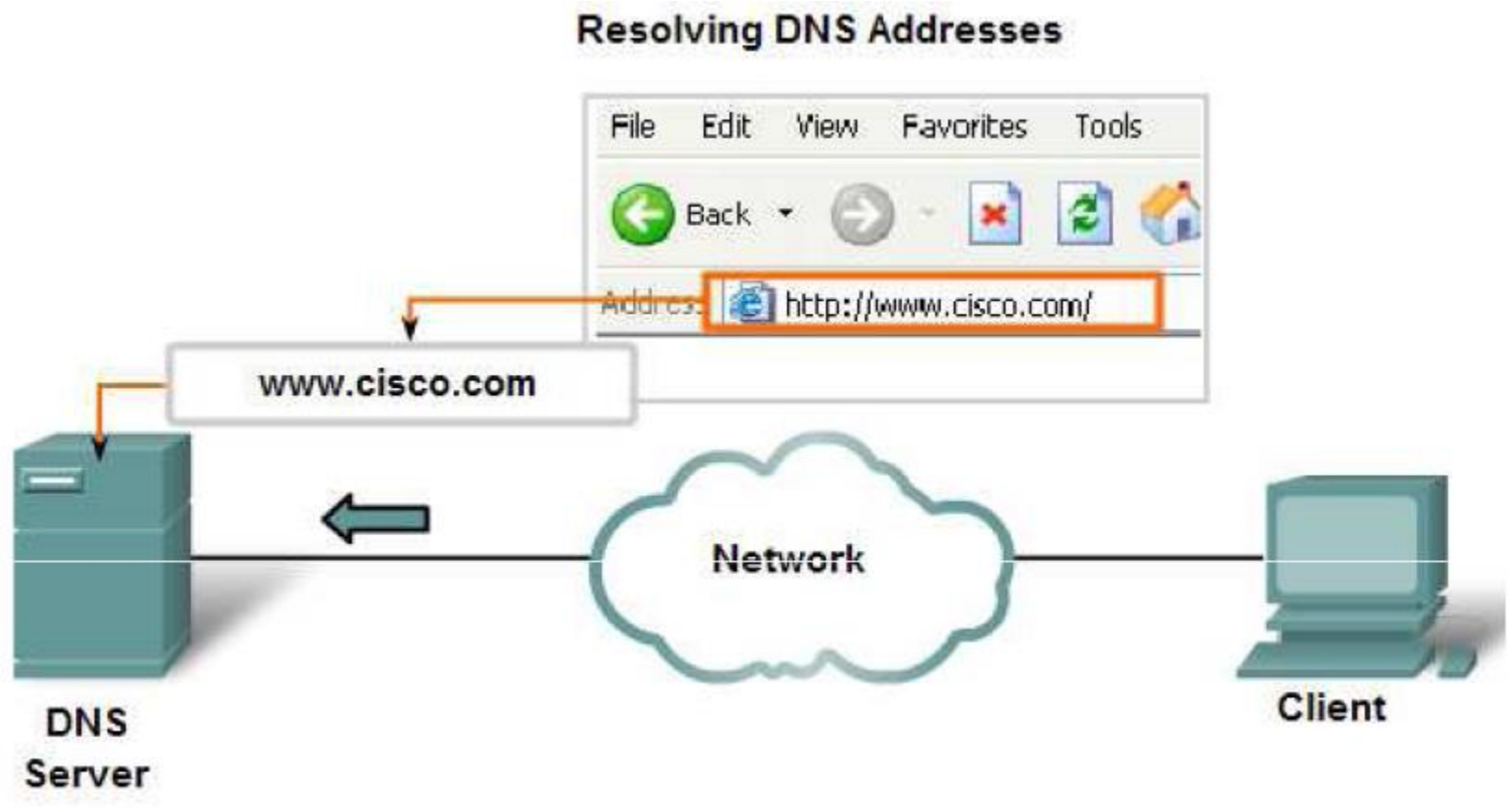
Example



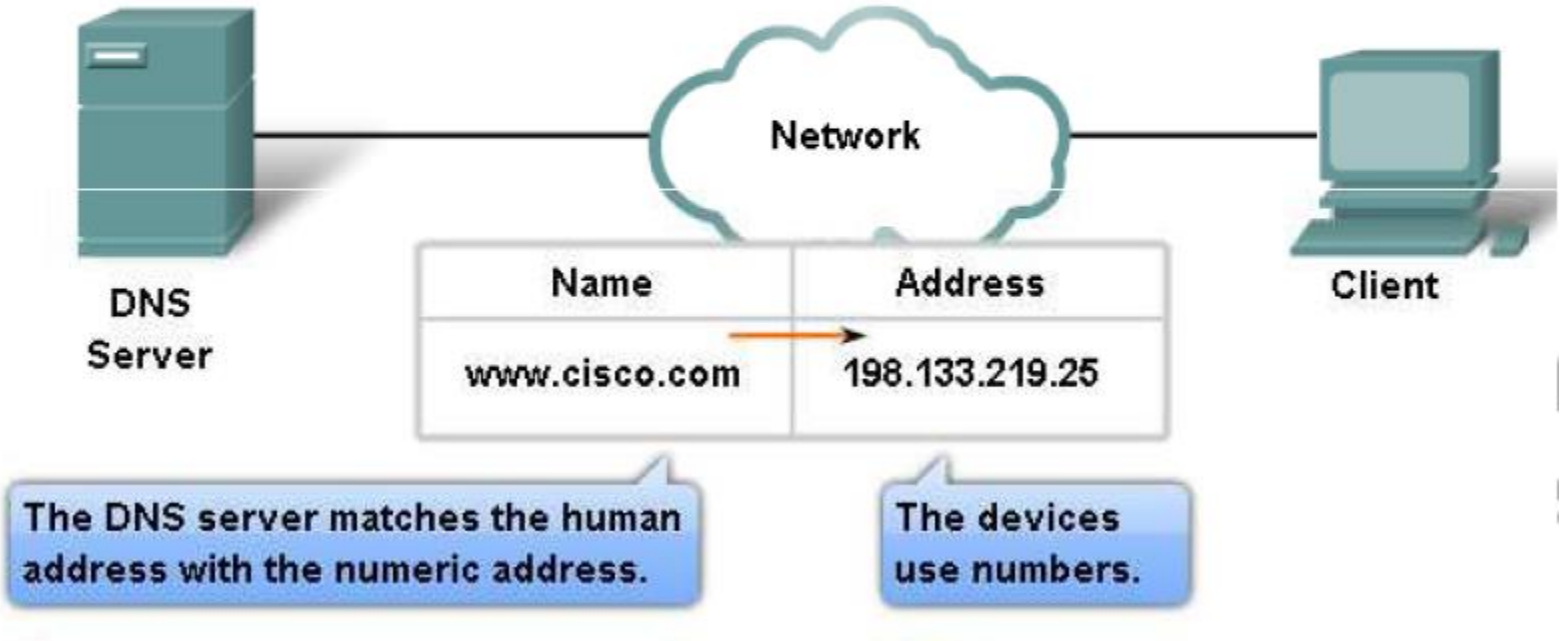
Example


Resolving DNS Addresses
File Edit View Favorites Tools
Back
Address
http://www.cisco.com/
The name is easy for people to use.
Network
DNS Server
Client

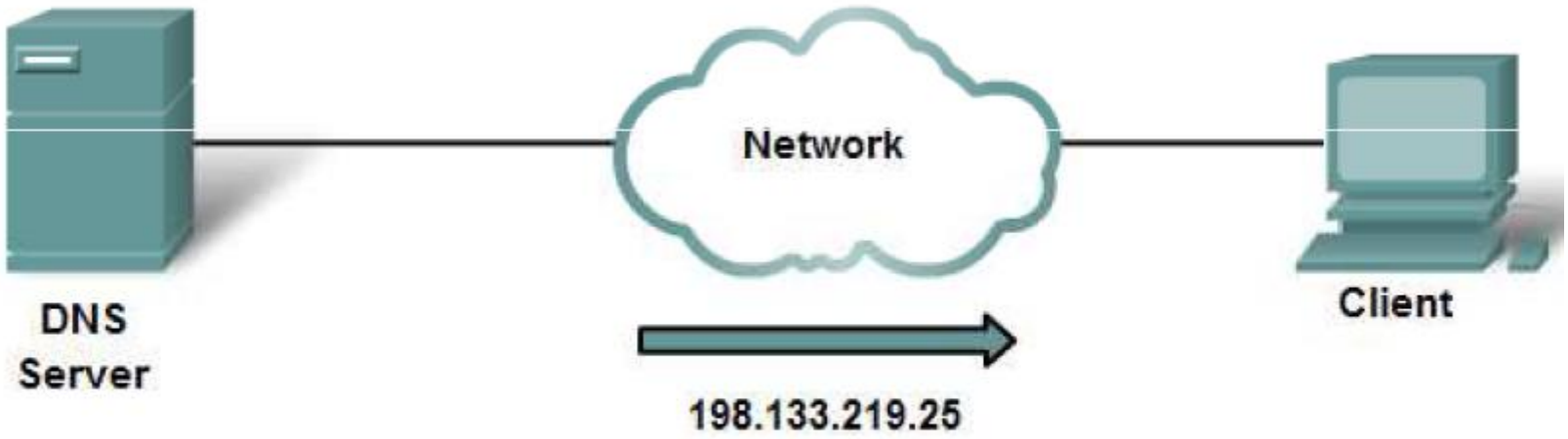
Example


Resolving DNS Addresses
File
Edit
View
Favorites
Tools
Back
http://www.cisco.com/
www.cisco.com
Network
DNS
Server
Client

Example

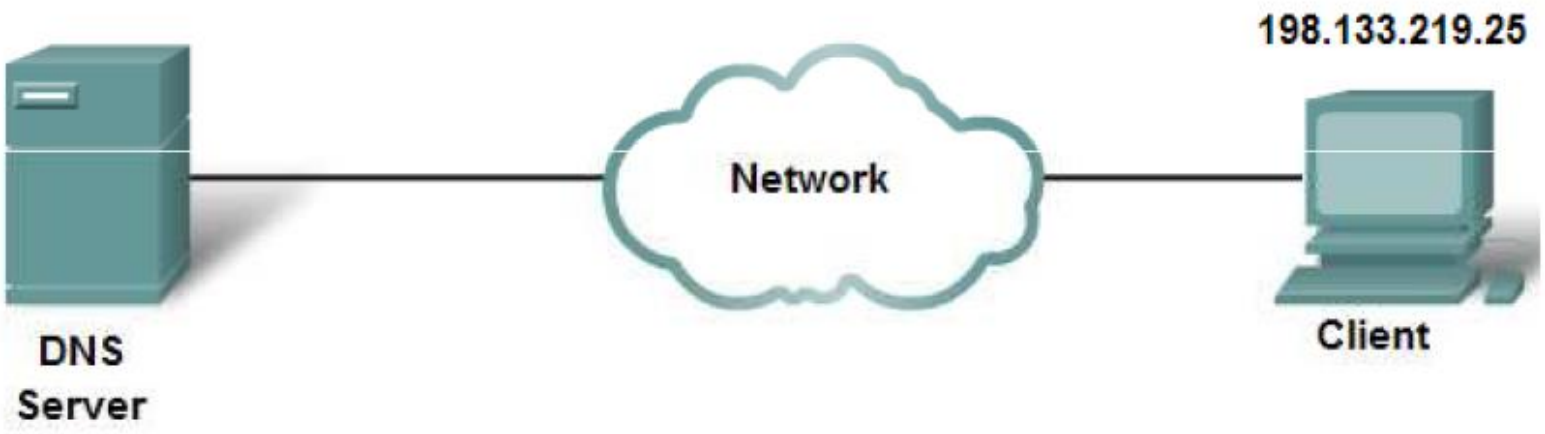

Network
DNS
Server
Name
Address
www.cisco.com
198.133.219.25
Client
The DNS server matches the human address with the numeric address.
The devices use numbers.

Example



The number is returned back to the client for use in making requests of the server.

Example



A human legible name is resolved to its numeric network device address by the DNS protocol.

HTTP/WWW

HTTP/WWW

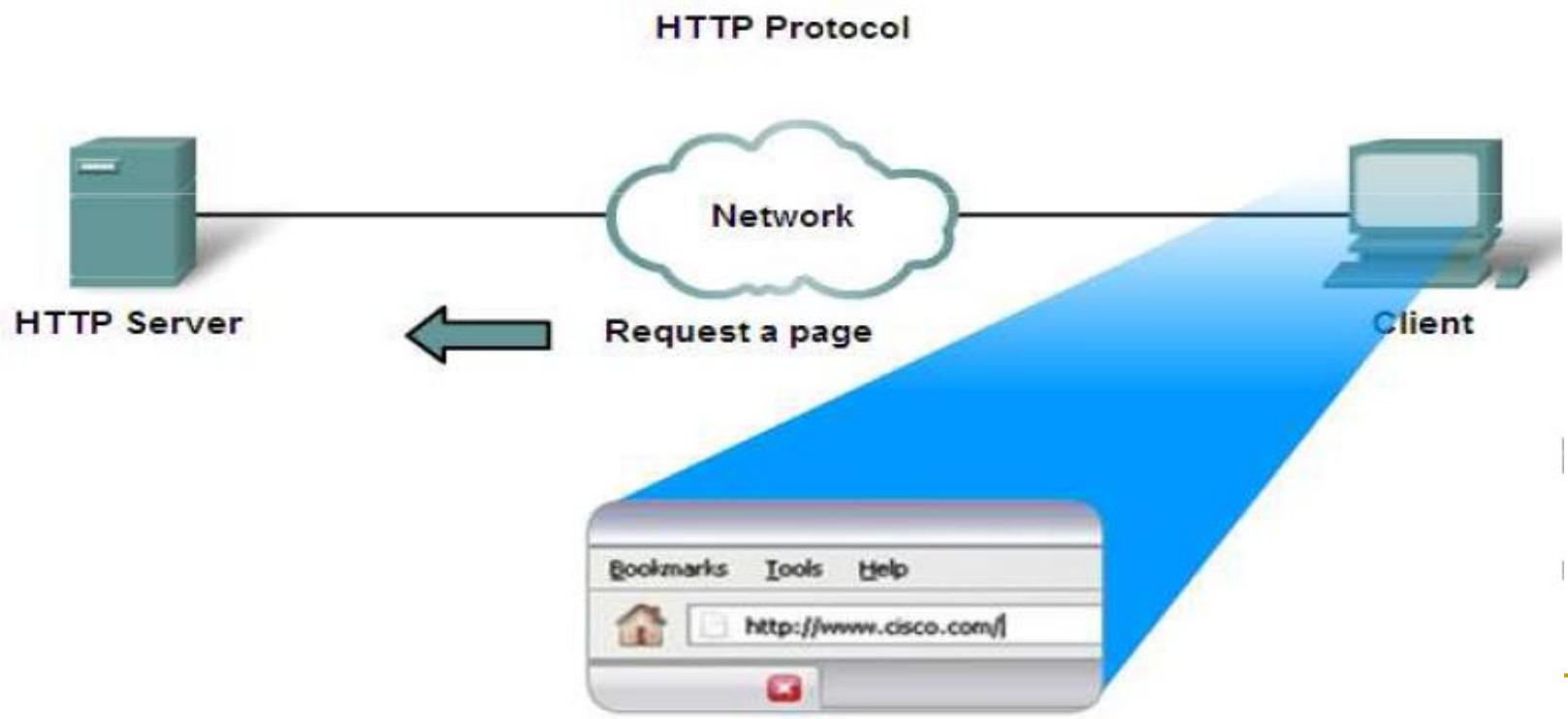
- The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web (WWW).

HTTP/WWW

- HTTP functions as a request-response protocol in the client-server computing model.
  - Clients: web browsers
  - Server: an application running on a computer hosting a web site

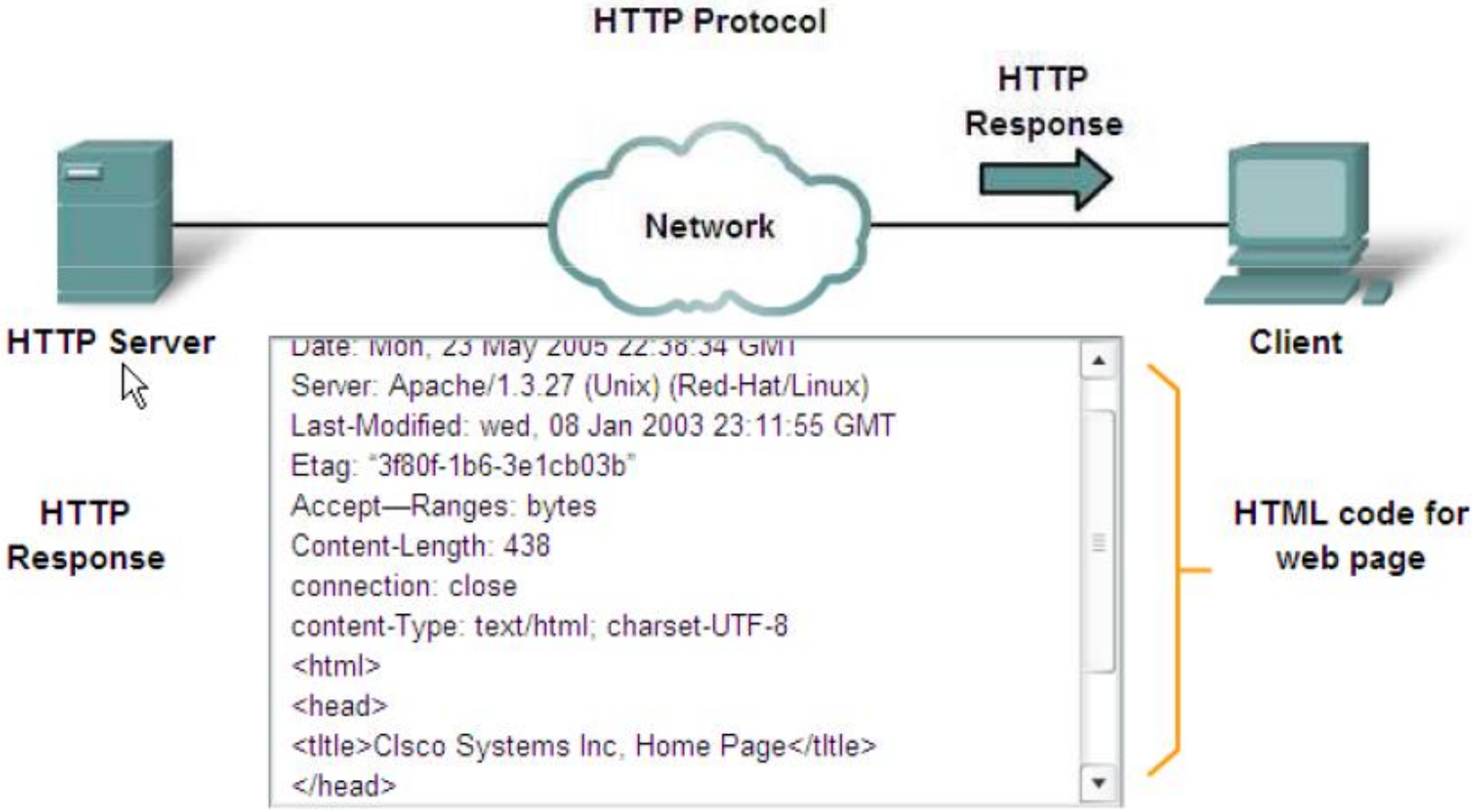
HTTP/WWW: Example

When you type a website address into web browser, web browser will establish connection with web server using HTTP protocol.



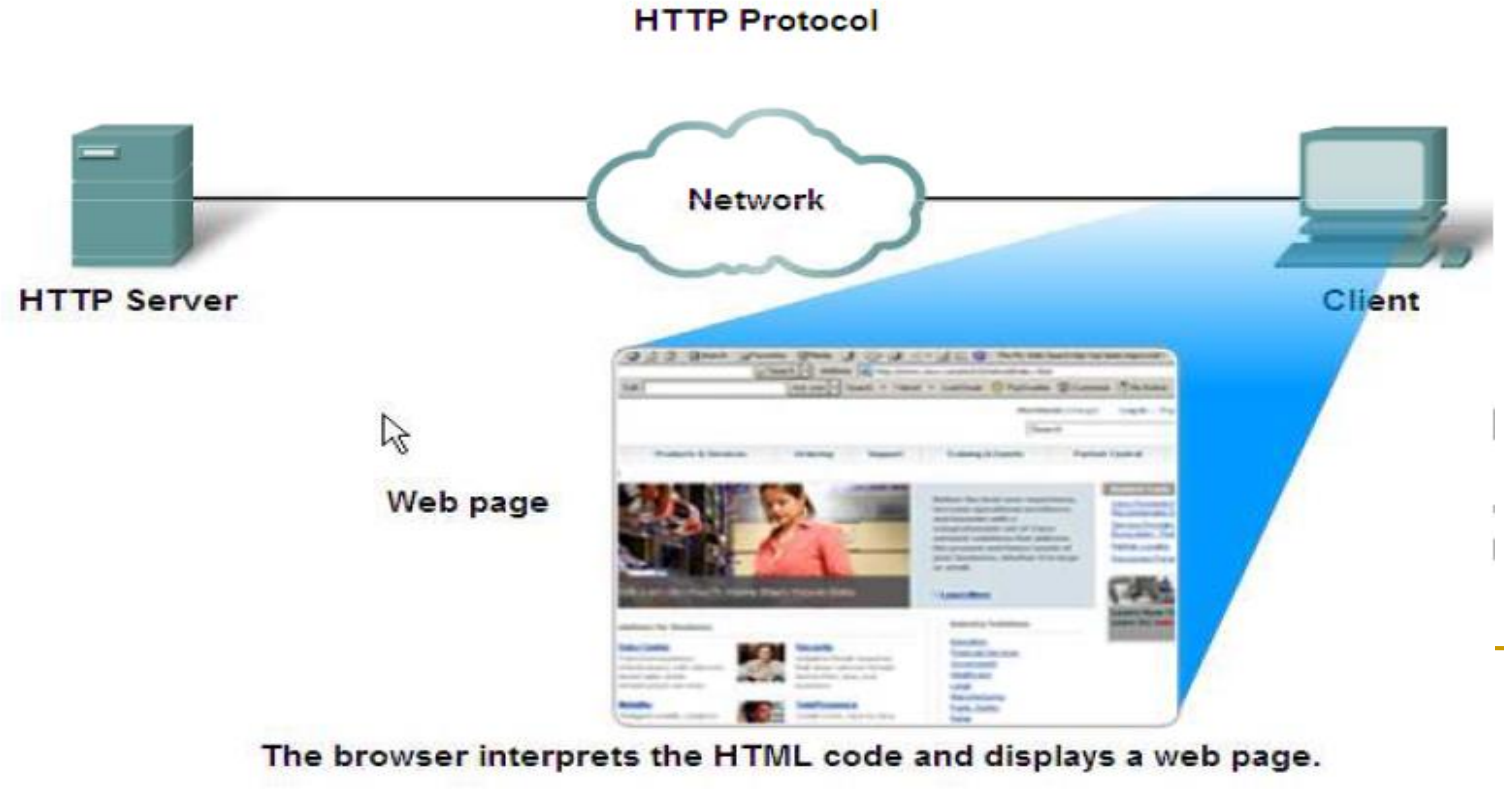
HTTP/WWW: Example

- Web server sends “HTTP response” back to web client.



HTTP/WWW: Example

- Web browser (client) can display many types of data, including HTML (Hypertext Markup Language).



Email and SMTP/POP

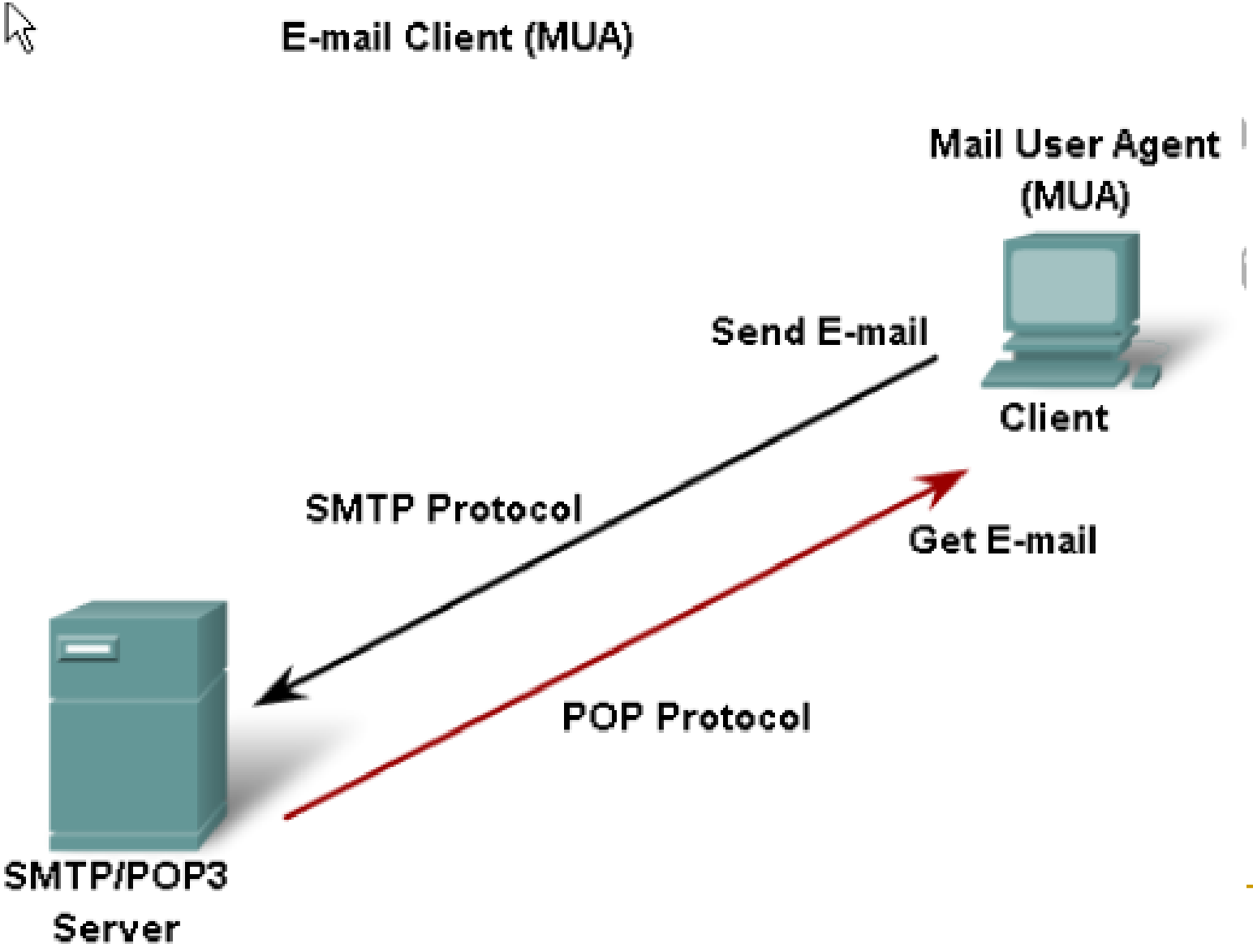
Email and SMTP/POP

- E-mail is the most popular network service nowaday.
- SMTP is a delivery protocol only. It cannot pull messages from a remote server on demand. Other protocols, such as the Post Office Protocol(POP) and the Internet Message Access Protocol (IMAP) are specifically designed for retrieving messages and managing mail boxes.

Email and SMTP/POP

- POP/SMTP: protocols used to send/receive mail.
- POP : is protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
- Mail User Agent (MUA) : is email client used to access and manage a user's email.

Email and SMTP/POP



FTP

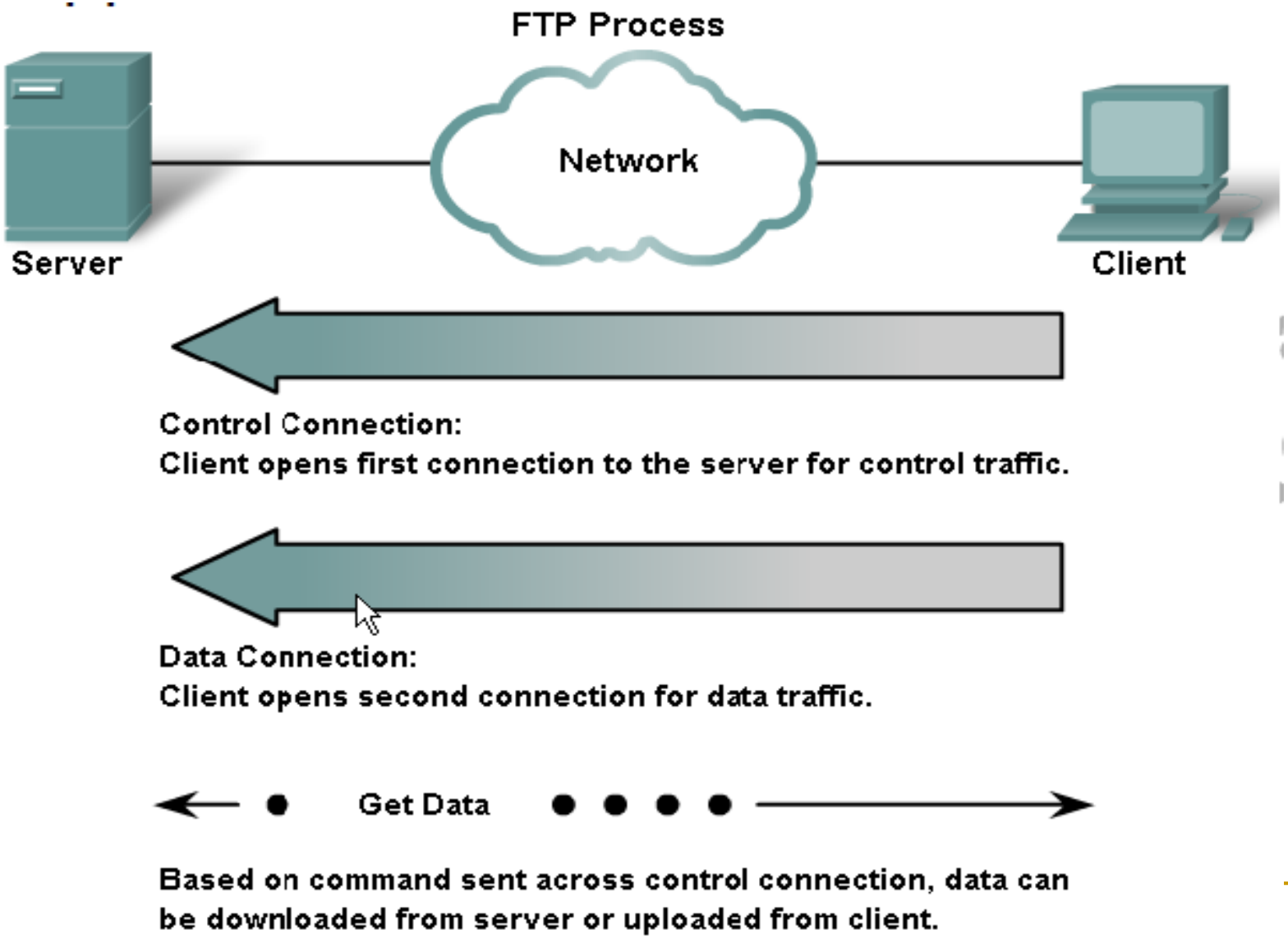
FTP

- FTP is a standard network protocol used to transfer files from one host to another host over a TCP-based network.
- FTP operates on the application layer of the OSI model, and is used to transfer files using TCP/IP

FTP

- FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.
  - Control connection: FTP server has to be running and waiting for incoming requests. The client computer is then able to communicate with the server on port 21.
  - Data connection: second connection can either be opened by the server from its port 20 to a negotiated client port (active mode), or by the client from an arbitrary port to a negotiated server port (passive mode) as required to transfer file data

FTP

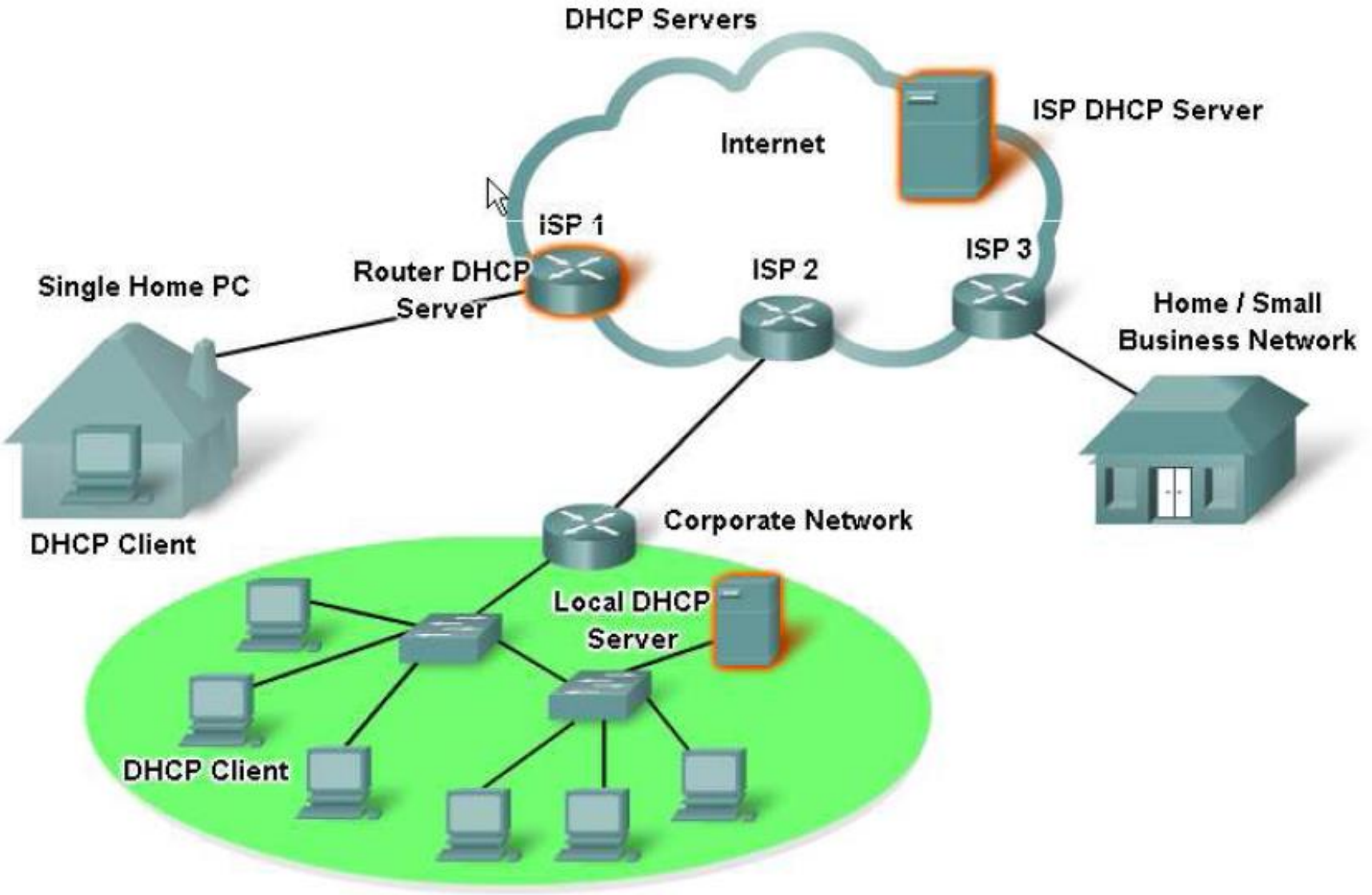

FTP Process
Network
Server
Client
Control Connection:
Client opens first connection to the server for control traffic.
Data Connection:
Client opens second connection for data traffic.
Get Data
Based on command sent across control connection, data can be downloaded from server or uploaded from client.

DHCP/DHCPv6

DHCP

- DHCP (Dynamic Host Configuration Protocol) provides configuration parameters to Internet hosts
- DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts

DHCP


DHCP Servers
Internet
ISP DHCP Server
ISP 1
ISP 2
ISP 3
Router DHCP Server
Single Home PC
Home / Small Business Network
DHCP Client
Corporate Network
Local DHCP Server
DHCP Client

DHCP: advantage

- DHCP eliminates the manual task by a network administrator.
- DHCP provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.

NFS

NFS (Network File System)

- NFS is a distributed file system protocol originally developed by Sun Microsystems allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed.
- NFS is often used with Unix/Linux operating systems (mount/unmount commands)

SNMP

SNMP

- Simple Network Management protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.
- Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.

SNMP

- 2 components :
  - Managers : one or more administrative computers have the task of monitoring or managing a group of hosts or devices on a computer network.
  - Agent : Software is executed in each managed system which reports information via SNMP to the manager.

SNMP

- SNMP uses UDP to transfer information between managers and agents => SNMP can operate even when there are some problems in network connection.
- SNMP specifies some core protocol data units (PDUs). Managers and agents use these PDUs to exchange information.

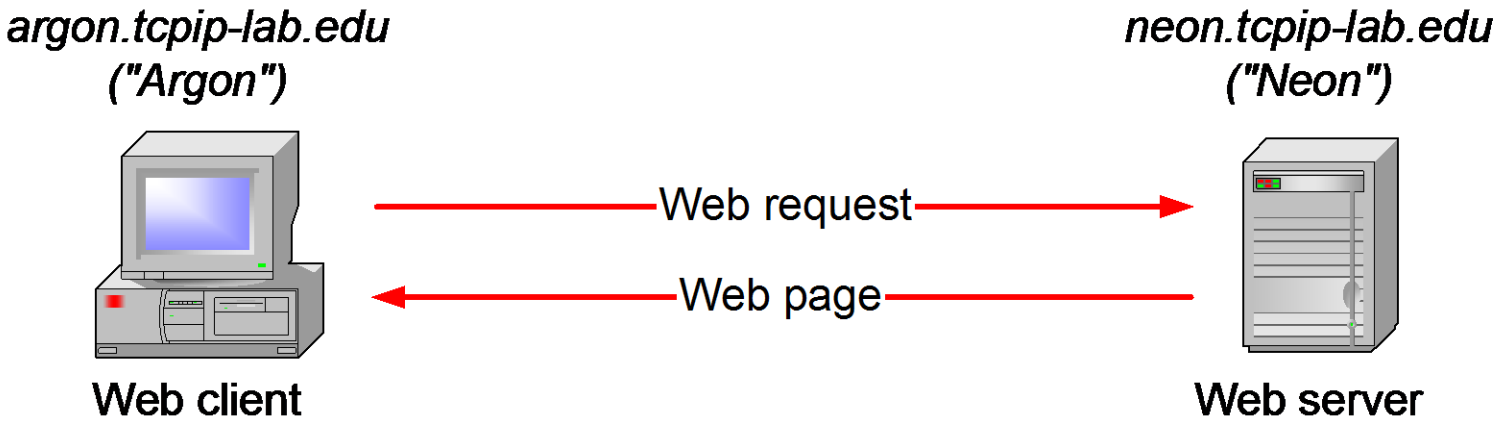
A simple TCP/IP example

- Source:
  - *www.cs.virginia.edu/~cs458/slides/module01-exampleV2.**ppt***

A simple TCP/IP Example

- A user on host *argon.tcpip-lab.edu* (“*Argon*”) makes a web access to URL

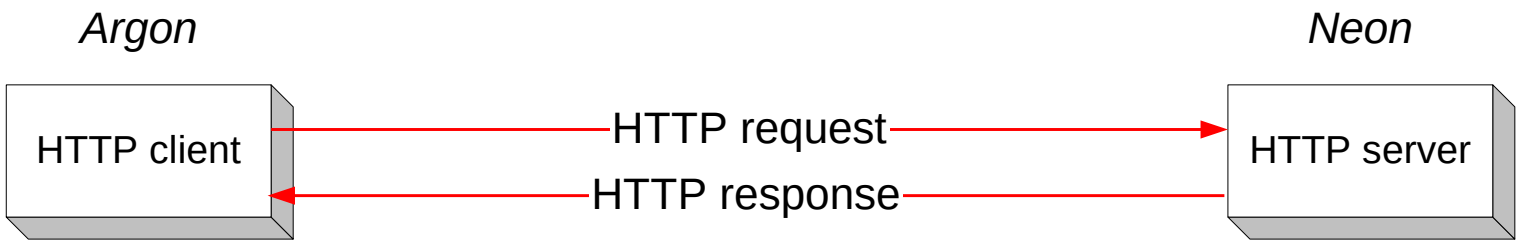
  http://neon.tcpip-lab.edu/index.html.



- What actually happens in the network?

HTTP Request and HTTP response

- Web browser runs an HTTP client program
- Web server runs an HTTP server program
- HTTP client sends an HTTP request to HTTP server
- HTTP server responds with HTTP response



HTTP Request

```
GET /index.html HTTP/1.1
Accept: image/gif, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host: neon.tcpip-lab.edu
Connection: Keep-Alive
```

HTTP Response

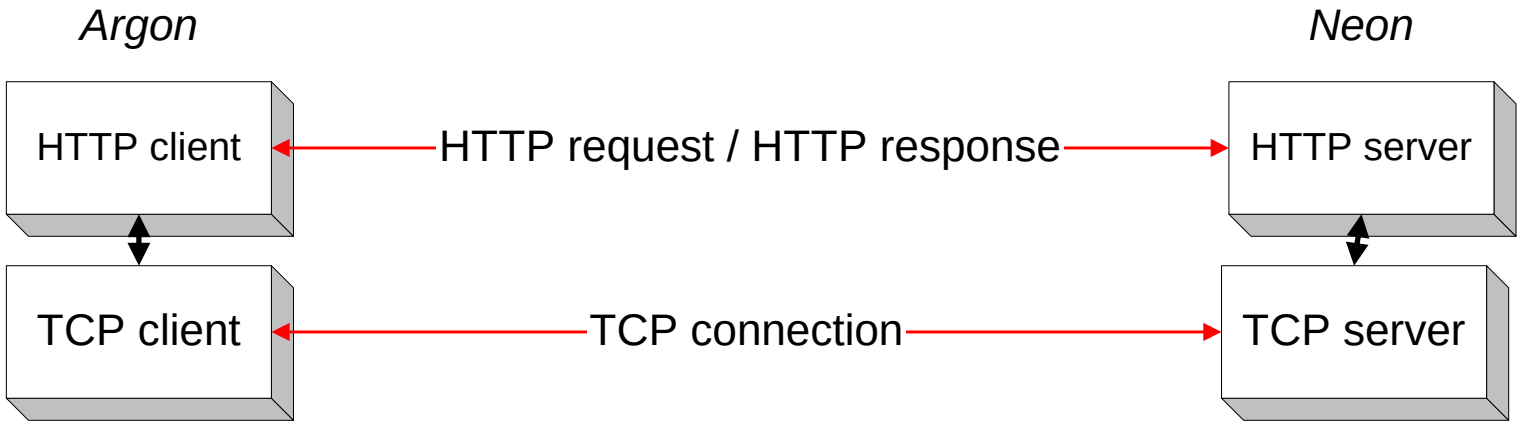
```
HTTP/1.1 200 OK
Date: Sat, 25 May 2002 21:10:32 GMT
Server: Apache/1.3.19 (Unix)
Last-Modified: Sat, 25 May 2002 20:51:33 GMT
ETag: "56497-51-3ceff955"
Accept-Ranges: bytes
Content-Length: 81
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<HTML>
<BODY>
<H1>Internet Lab</H1>
Click <a href="http://www.tcpip-
lab.net/index.html">here</a> for the Internet Lab webpage.
</BODY>
</HTML>
```

- How does the HTTP request get from Argon to Neon ?

From HTTP to TCP

- To send request, HTTP client program establishes an TCP connection to the HTTP server Neon.
- The HTTP server at Neon has a TCP server running



Resolving hostnames and port numbers

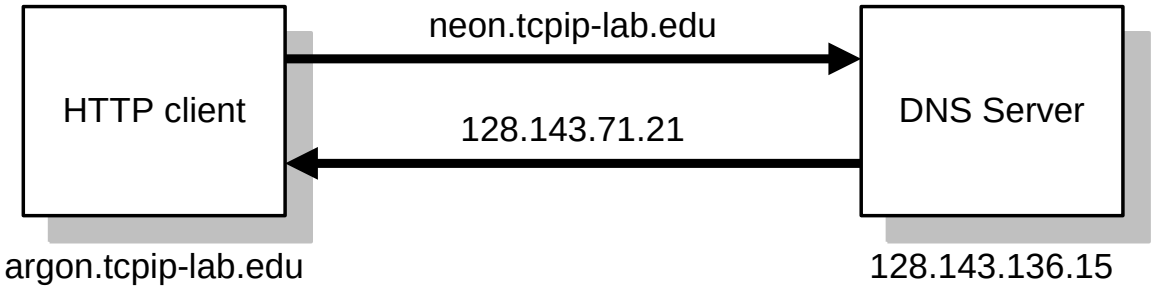
- Since TCP does not work with hostnames and also would not know how to find the HTTP server program at Neon, two things must happen:

    1. The name “neon.tcpip-lab.edu” must be translated into a 32-bit **IP address.**

    2. The HTTP server at Neon must be identified by a 16-bit **port number**.

Translating a hostname into an IP address

- The translation of the hostname *neon.tcpip-lab.edu* into an IP address is done via a database lookup



- The distributed database used is called the ***Domain Name System (DNS)***
- All machines on the Internet have an IP address:

argon.tcpip-lab.edu
128.143.137.144
neon.tcpip-lab.edu *128.143.71.21*

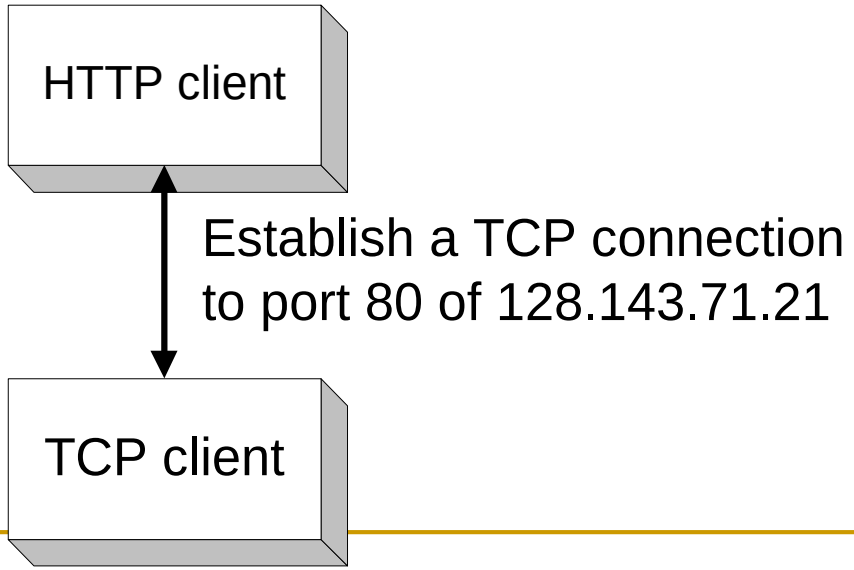
Finding the port number

- **Note:** Most services on the Internet are reachable via well-known ports. E.g. All HTTP servers on the Internet can be reached at port number “80”.
- **So:** Argon simply knows the port number of the HTTP server at a remote machine.
- On most Unix systems, the well-known ports are listed in a file with name /etc/services. The well-known port numbers of some of the most popular services are:

ftp	21	finger	79
telnet	23	http	80
smtp	25	nntp	119

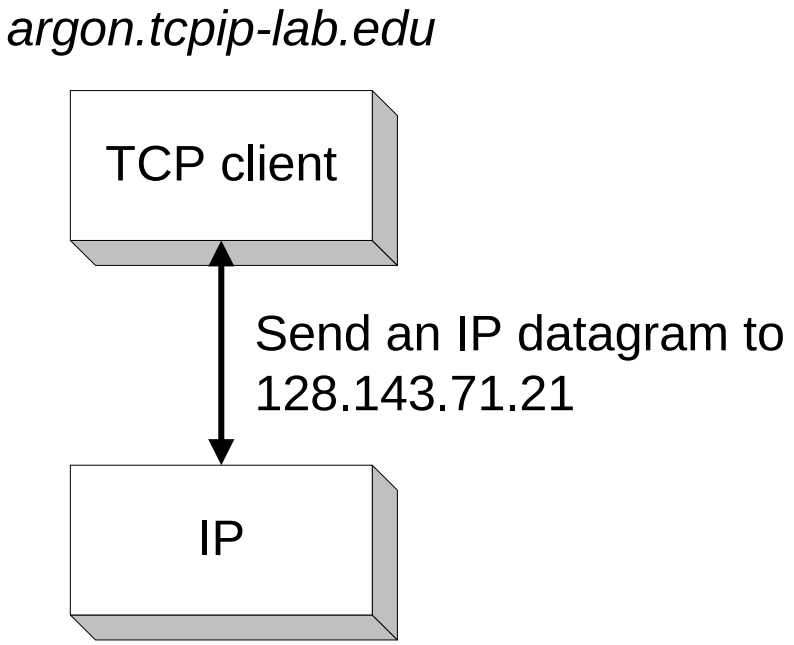
Requesting a TCP Connection

- The HTTP client at *argon.tcpip-lab.edu* requests the TCP client to establish a connection to port 80 of the machine with address 128.141.71.21



Invoking the IP Protocol

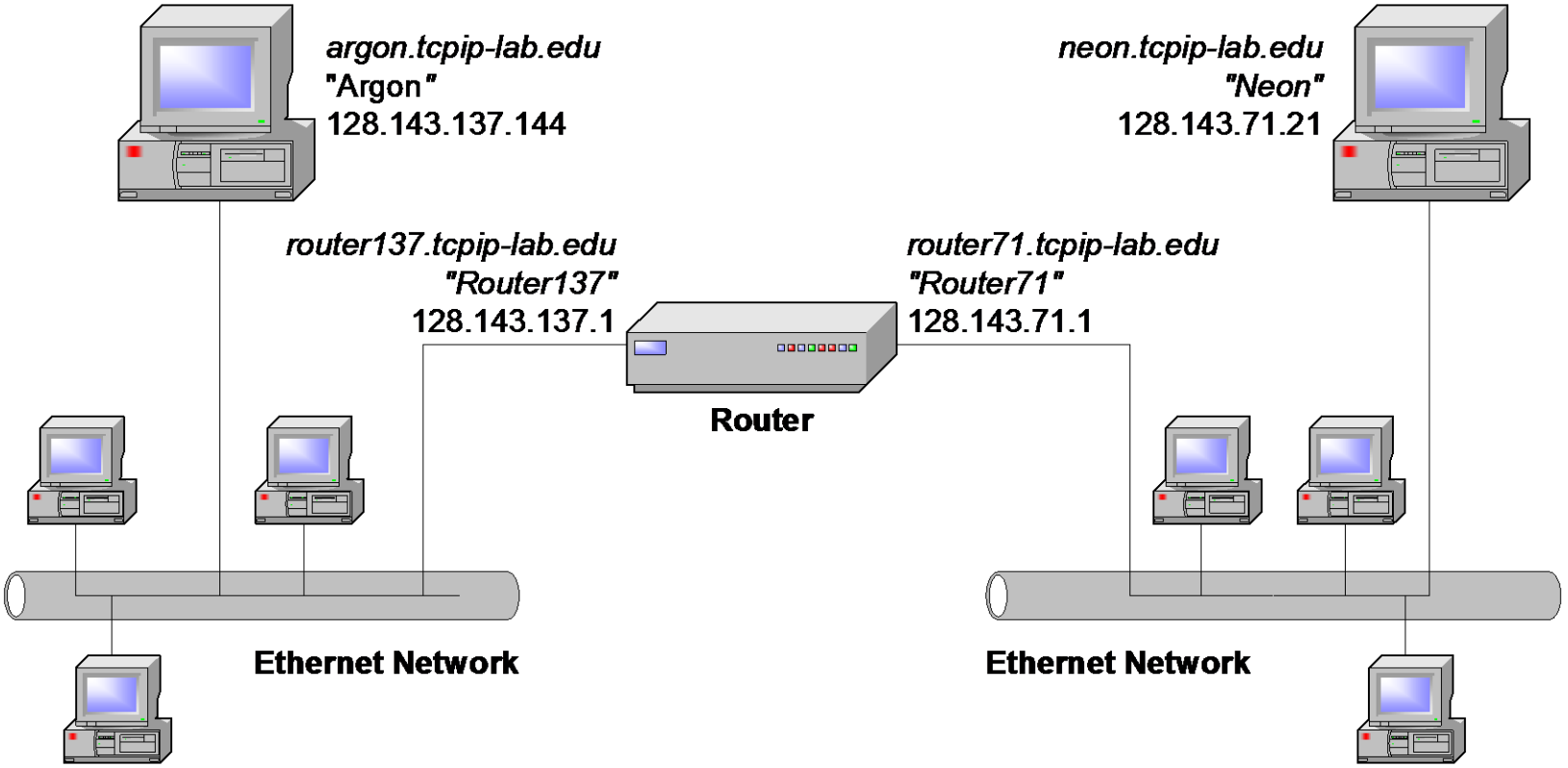
- The TCP client at *Argon* sends a request to establish a connection to port 80 at *Neon*
- This is done by asking its local IP module to send an IP datagram to *128.143.71.21*
- *(The data portion of the IP datagram contains the request to open a connection)*



Sending the IP datagram to an IP router

- *Argon (128.143.137.144)* can deliver the IP datagram directly to *Neon (128.143.71.21*), only if it is on the same local network ("subnet")
- But *Argon* and N*eon* are not on the same local network
  (**Q**: How does *Argon* know this?)
- So, *Argon* sends the IP datagram to its default gateway
- The default gateway is an IP router
- The default gateway for *Argon* is *Router137.tcpip-lab.edu* (128.143.137.1).

The route from *Argon* to *Neon*

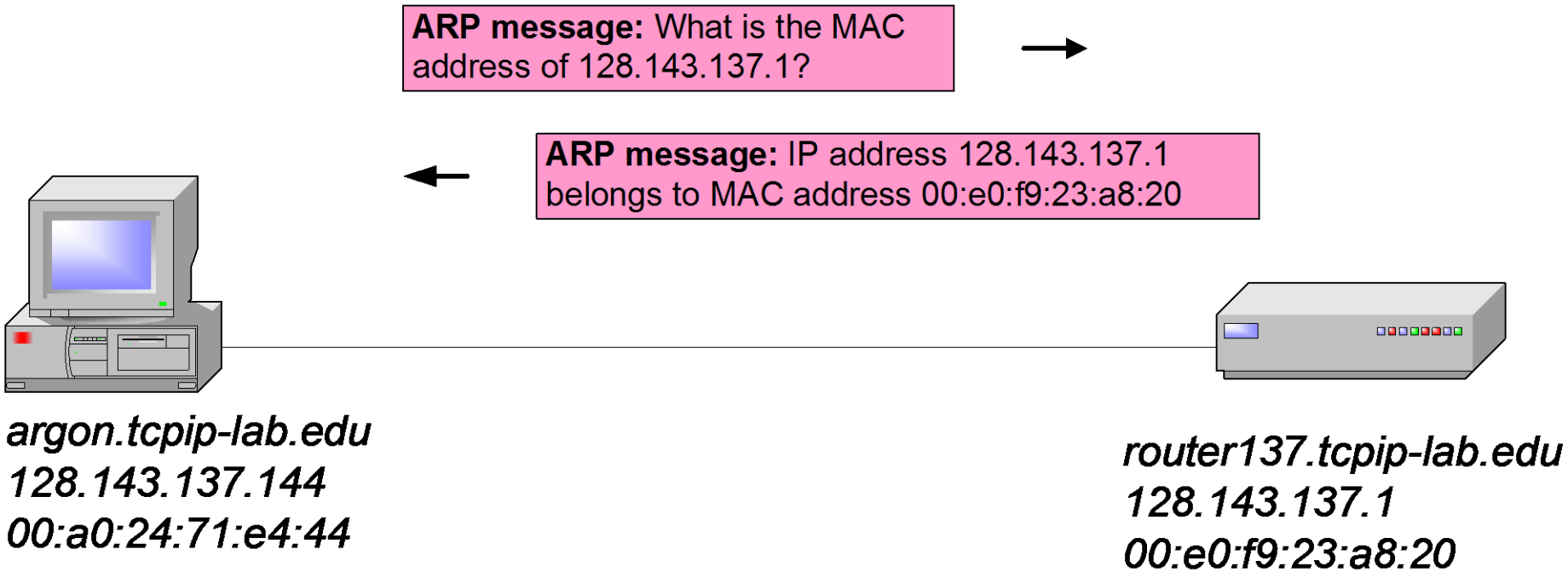


- Note that the gateway has a different name for each of its interfaces.

Finding the MAC address of the gateway

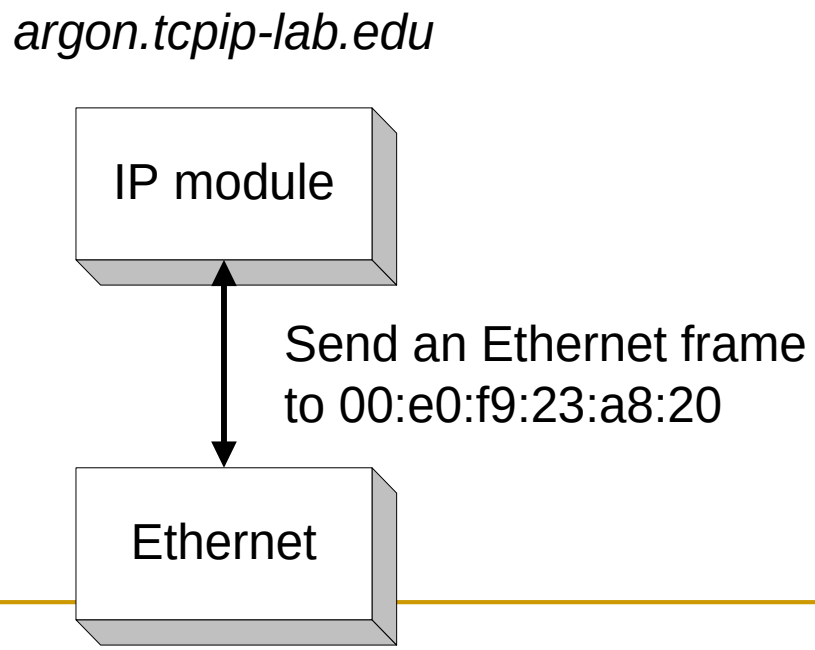
- To send an IP datagram to Router137, *Argon* puts the IP datagram in an Ethernet frame, and transmits the frame.
- However, Ethernet uses different addresses, so-called Media Access Control (MAC) addresses (also called: physical address, hardware address)
- Therefore, *Argon* must first translate the IP address 128.143.137.1 into a MAC address.
- The translation of addressed is performed via the Address Resolution Protocol (ARP)

Address resolution with ARP



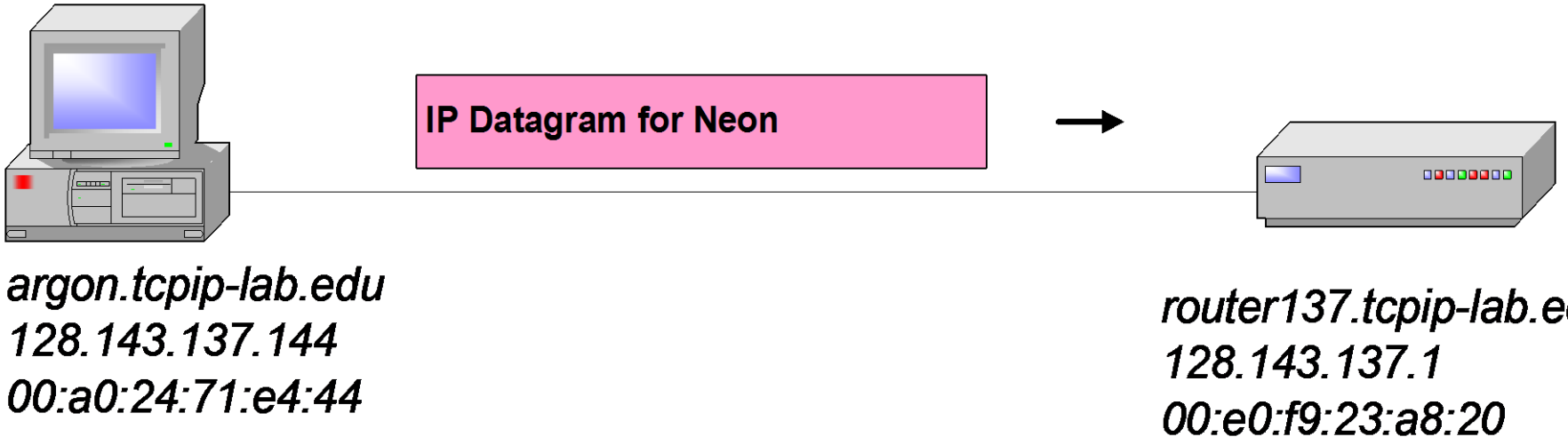
Invoking the device driver

- The IP module at *Argon*, tells its Ethernet device driver to send an Ethernet frame to address *00:e0:f9:23:a8:20*



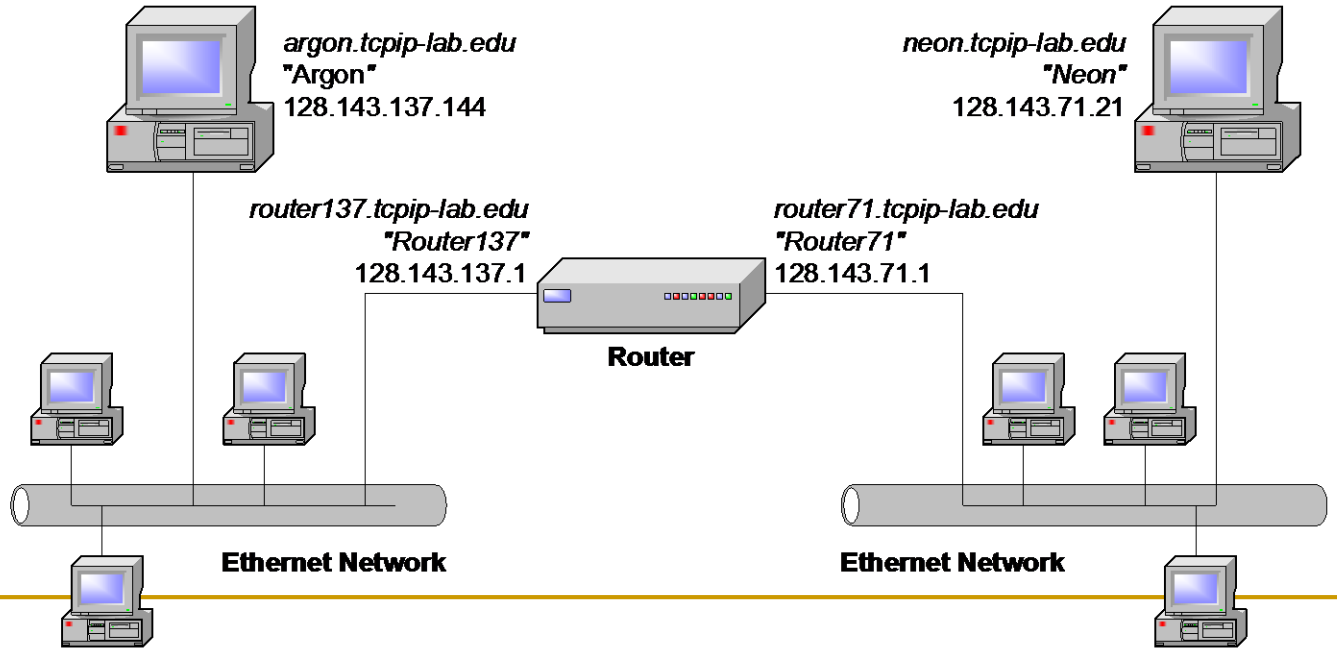
Sending an Ethernet frame

- The Ethernet device driver of *Argon* sends the Ethernet frame to the Ethernet network interface card (NIC)
- The NIC sends the frame onto the wire



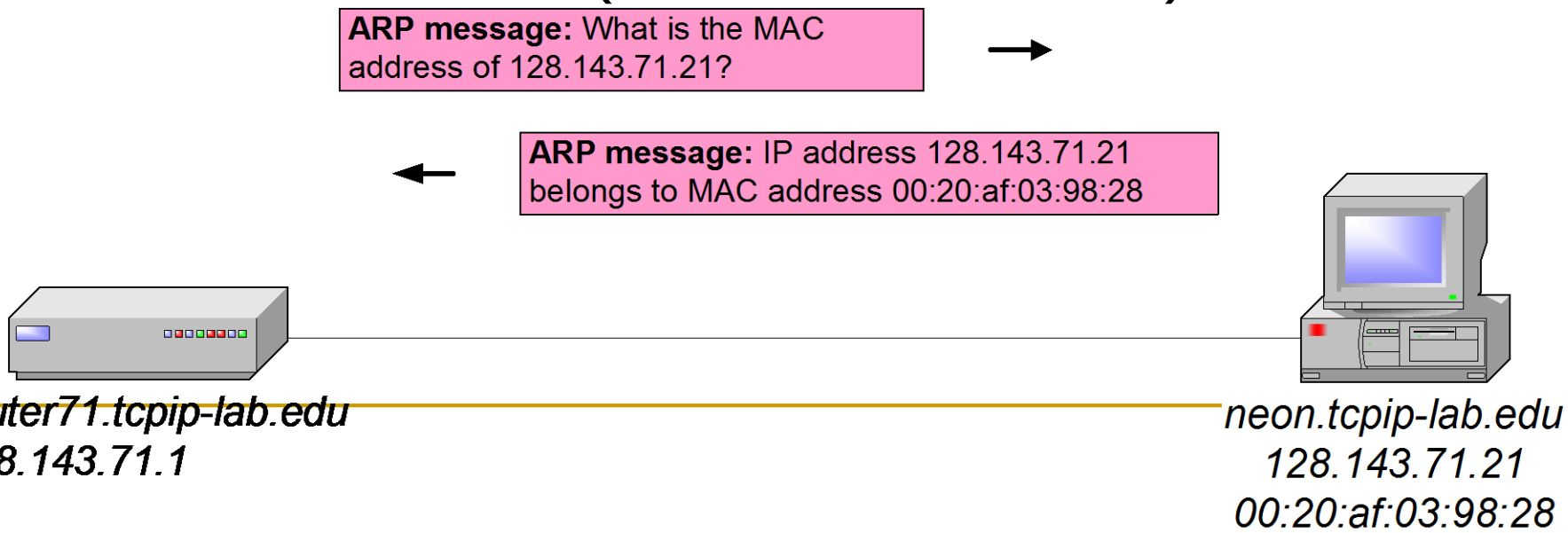
Forwarding the IP datagram

- The IP router receives the Ethernet frame at interface 128.143.137.1, recovers the IP datagram and determines that the IP datagram should be forwarded to the interface with name 128.143.71.1
- The IP router determines that it can deliver the IP datagram directly



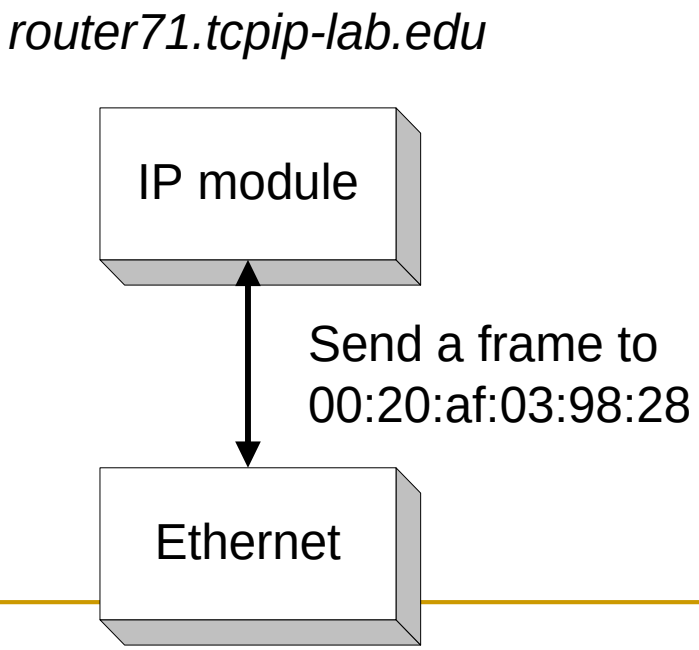
Another lookup of a MAC address

- The rouer needs to find the MAC address of *Neon*.
- Again, ARP is invoked, to translate the IP address of *Neon* (128.143.71.21) into the MAC address of neon (00:20:af:03:98:28).



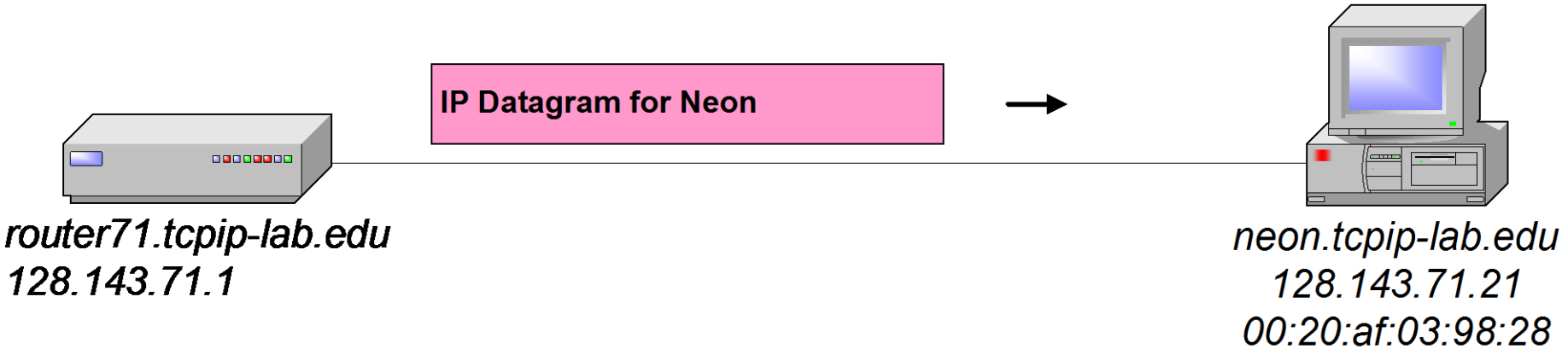
Invoking the device driver at the router

- The IP protocol at *Router71*, tells its Ethernet device driver to send an Ethernet frame to address *00:20:af:03:98:28*



Sending another Ethernet frame

- The Ethernet device driver of *Router71* sends the Ethernet frame to the Ethernet NIC, which transmits the frame onto the wire.



Data has arrived at Neon

- *Neon* receives the Ethernet frame
- The payload of the Ethernet frame is an IP datagram which is passed to the IP protocol.
- The payload of the IP datagram is a TCP segment, which is passed to the TCP server
- **Note**: Since the TCP segment is a connection request (SYN), the TCP protocol does not pass data to the HTTP program for this packet. Instead, the TCP protocol at neon will respond with a SYN segment to *Argon*.