

TCP/IP Reference Models and Overview

Presented By
Dr. Md. Abir Hossain

TCP/IP

- A highly standardized protocol used widely on the Internet
- Standards area available in the form of RFC documents
 - [Request For Comments \(RFC\)](#)
- Standards are overseen by the [Internet Engineering Task Force](#) (IETF)

Layers of TCP/IP Reference Model

- There are four layers of the TCP/IP reference model (DARPA model as named by the US Government Agency)
 - The ISO-OSI reference model is composed of seven layers
- The next slide shows the mapping of the ISO/OSI model to the TCP/IP model
- Note that the ISO/OSI model is more widely used and accepted but the TCP/IP model is easy to comprehend

ISO-OSI Seven Layer Model Recalled

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Source: <http://starter.sdsu.edu/remote/demo/osi-tcp.html>

Comparison of ISO-OSI Model and the DOD (TCP/IP) Model

Source: <http://starter.sdsu.edu/remote/demo/osi-tcp.html>

Application	
Presentation	Application
Session	
Transport	Host-to-Host
Network	Internet
Data Link	
Physical	Network Access

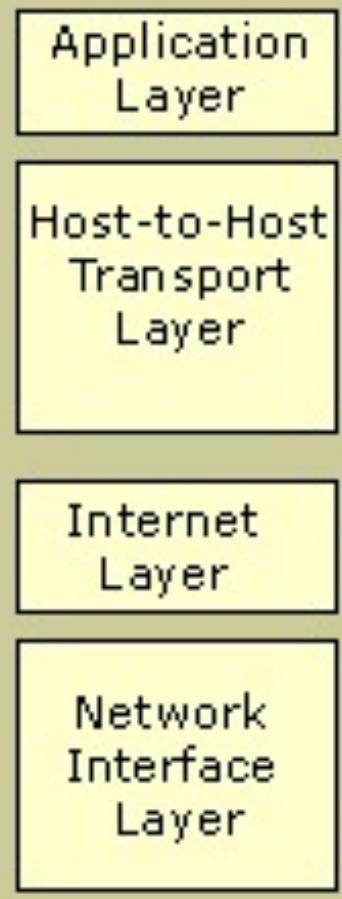
Layer Reference to Protocol

Application		
Presentation	Application	FTP, Telnet, SMTP, HTTP..
Session		
Transport	Host-to-Host	TCP, UDP
Network	Internet	IP, ICMP, IGMP
Data Link	Network Access	Ethernet, Token-Ring, PPP
Physical		

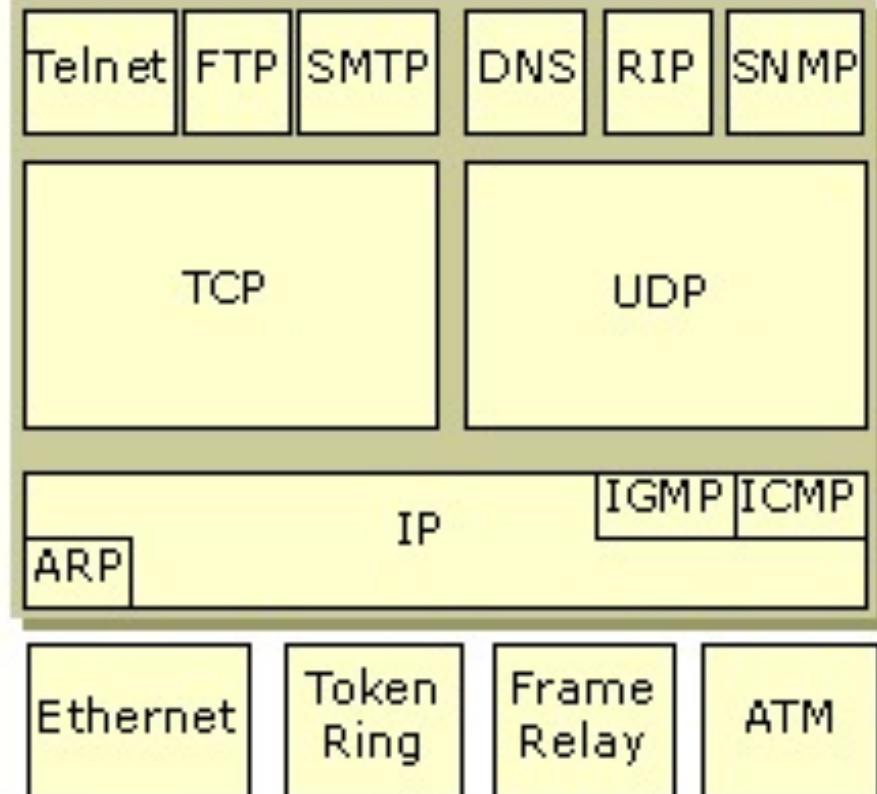
OSI Model Layers



TCP/IP Protocol Architecture Layers



TCP/IP Protocol Suite



TCP/IP Layers

- Network Access/interface layer
- Internet layer
- Host-to-host transport layer
- Application layer

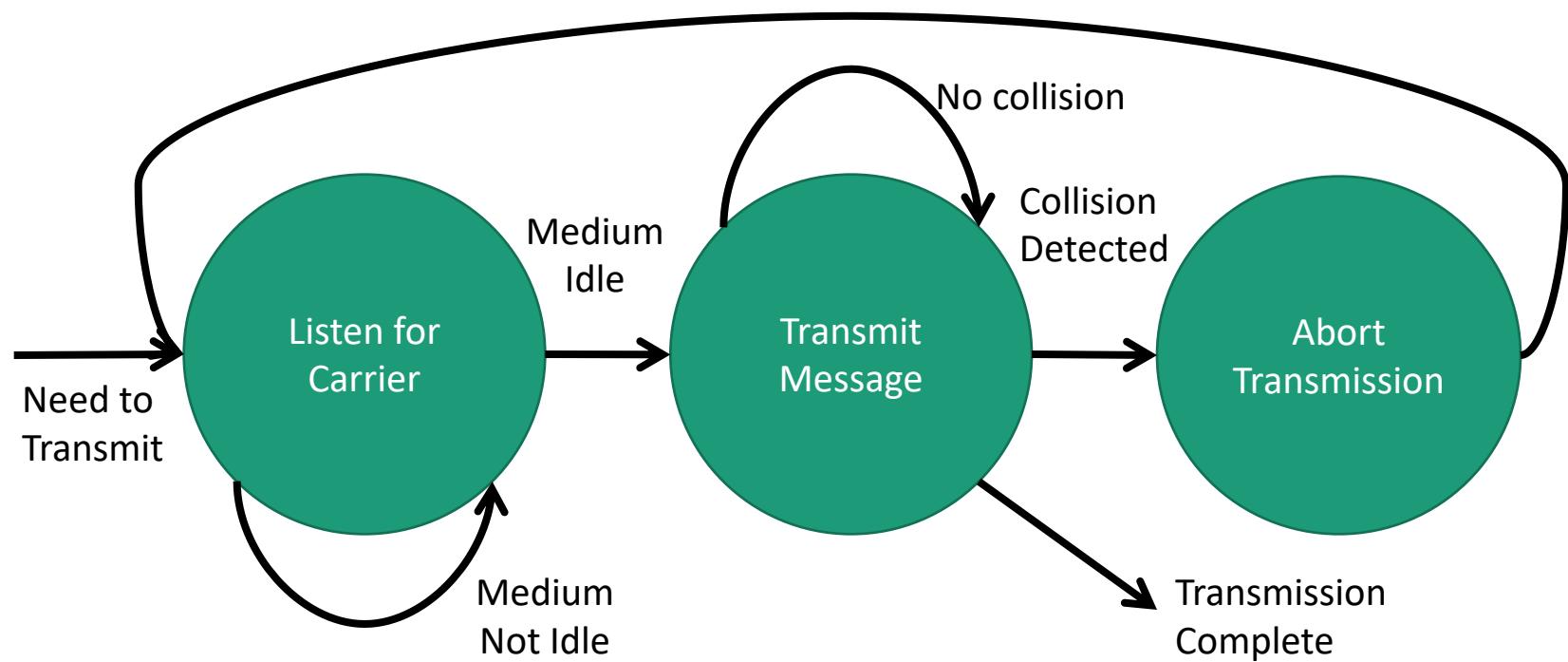
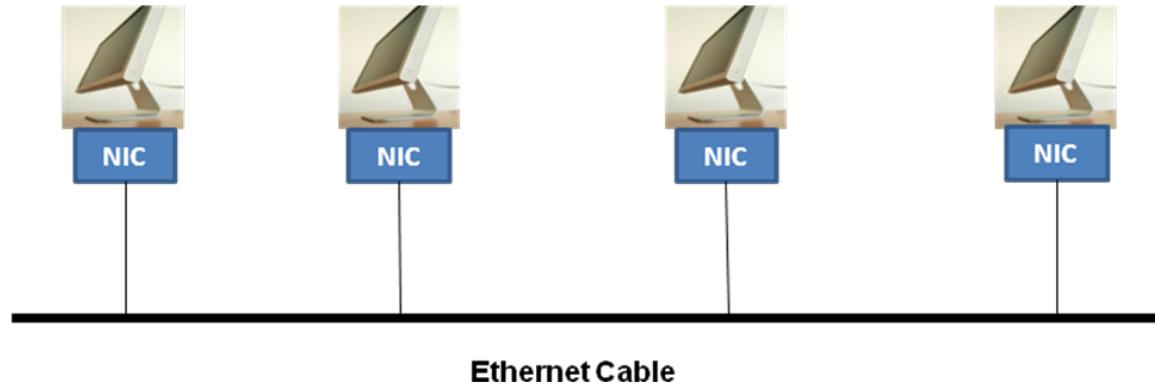
Network Interface Layer

- Responsible for sending and receiving TCP/IP packets on the network medium (physical/Data Link)
- Applicable LAN technologies
 - Ethernet, Token Ring, FDDI etc.
- Applicable WAN technologies
 - X.25 (old), Frame Relay, ATM etc.
- Note that some technologies such as ATM and FDDI may be used at both the WAN and the LAN levels

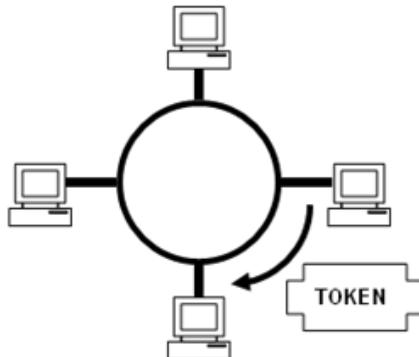
Some Core Protocols

- IEEE 802.3 (Ethernet LAN), IEEE 802.5 (Token Ring) and IEEE 802.11(Wireless LAN) series of protocols

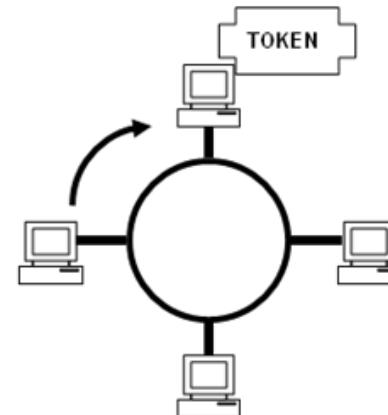
Ethernet



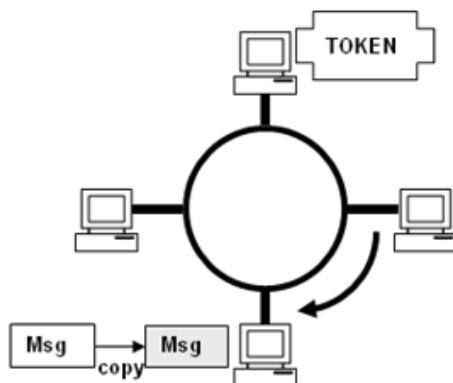
Token Ring



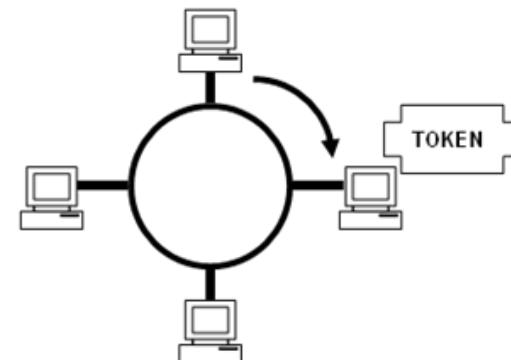
Token is passed from host to host....



....until it arrives at a host that has a message to send.



The host holding the token sends a message to the next host on the ring. Each host continues to pass the message to the next host. If a host is the intended recipient of the message it makes a copy but continues the process of sending to the next host. Message will continue to circulate until it returns to sender who will verify that the message is the same as the one sent, remove it, and resume token passing.



Token passing resumes

Comparison

Link Layer Protocol	Features	Pros	Cons
Ethernet	Member of random access protocol family; opportunistic broadcast using CSMA/CD; exponential backoff on collision	Simple to manage; works well in light load	Too many collisions under high load
Token ring	Member of taking turns protocol family; Token needed to transmit	Fair access to all competing stations; works well under heavy load	Unnecessary latency for token acquisition under light load

Other link layer protocols

- FDDI: Fiber Distributed Data Interface
 - Fiber optics based
 - High bandwidth backbone used to connect LAN's
 - FDDI was upstaged by Gigabit Ethernet
- ATM: Asynchronous Transfer Mode
 - Guarantees quality of service using link reservation and admission control to avoid congestion
 - Connection oriented and can have transport layer implemented on top of it
 - Used in MAN's and WAN's network
 - ATM is likely to be upstaged by 10-Gigabit Ethernet
- PPP: Point to Point Protocol
 - Transmit multiprotocol data
 - Used by dial-up connections
 - widely used in broadband communications

Internet Layer

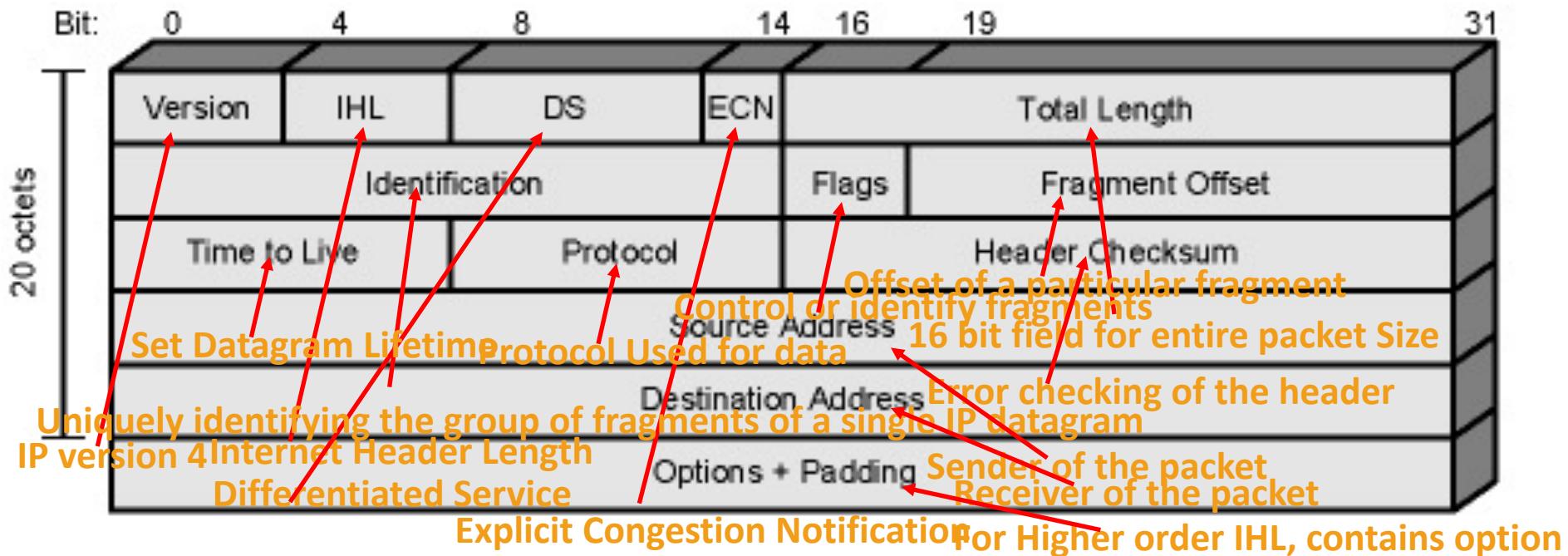
- Connectionless, point to point internetworking protocol (uses the datagram approach)
 - takes care of routing across multiple networks
 - each packet travels in the network independently of each other
 - they may not arrive (if there is a problem in the network)
 - a design decision enforced by DoD to make the system more flexible and responsive to loss of some subnet devices
- Implemented in end systems and routers as the Internet Protocol (IP)

Core Internet Layer Protocols

- IP
 - A connectionless unreliable protocol that is part of the TCP/IP protocol suite
- ARP (Address Resolution Protocol)
 - Resolves IP addresses to MAC addresses
- ICMP (Internet Control Message Protocol)
 - Diagnostics and error reporting
- (IGMP) Internet Group Management Protocol
 - Management of group multicast

IP (Internet Protocol)

- The core of the TCP/IP protocol suite
- Two versions co-exist
 - v4 – the widely used IP protocol
 - v6 – has been standardized in 1996, but still not widely deployed
- IP (v4) header minimum 20 octets (160 bits)



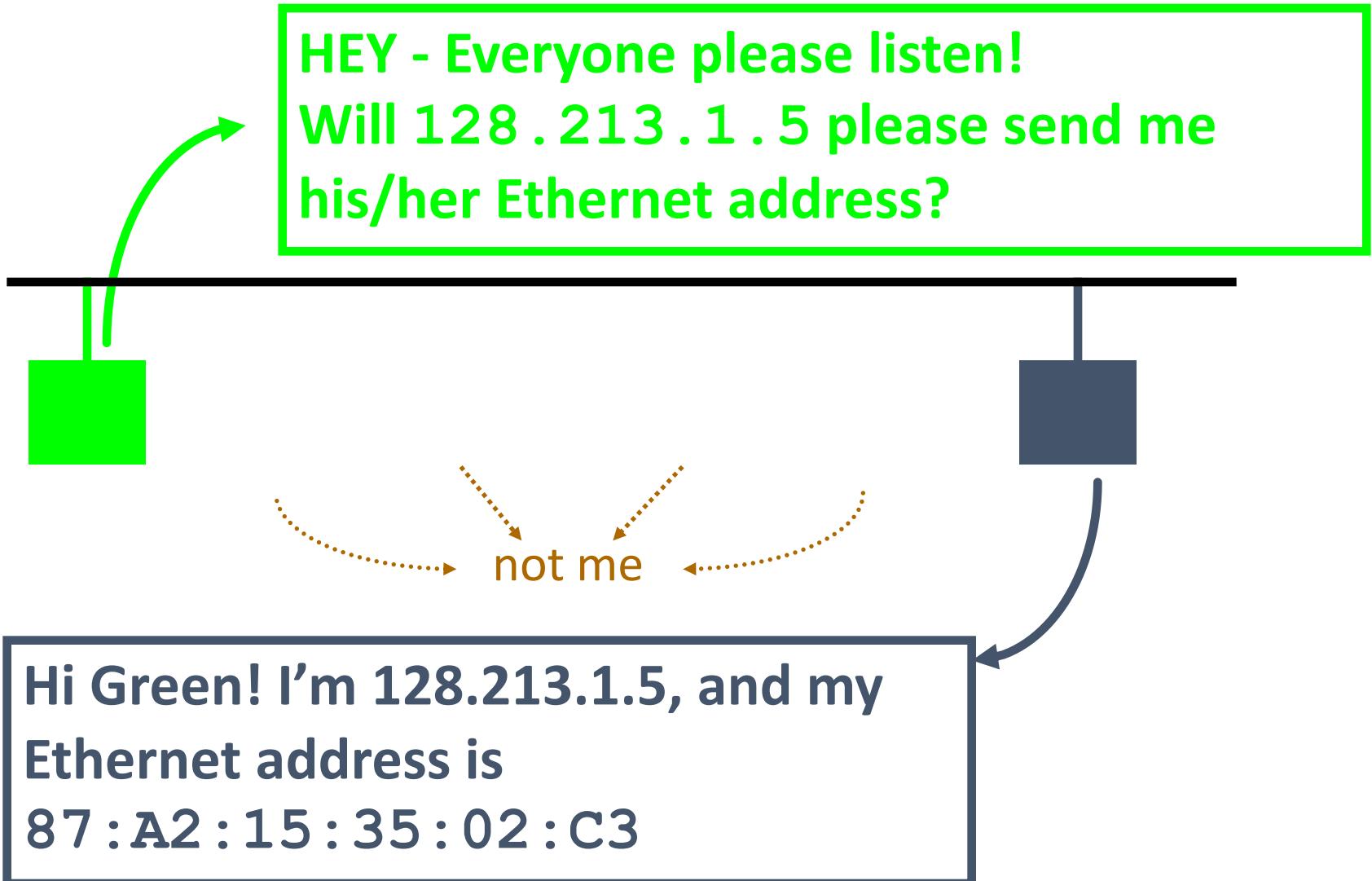
IPv6

- IPv6
 - Enhancements over IPv4 for modern high speed networks
 - Support for multimedia data streams
- But the driving force behind v6 was to increase address space
 - 128-bit as compared to 32-bit of v4
- Not backward compatible
 - all equipment and software must change

Address Resolution Protocol (ARP)

- ARP is a protocol used for finding link layer addresses from network layer addresses.
- It usually determine 48-bit Ethernet address from a 32-bit IP address.
- ARP uses the broadcast mechanism to try to find a host's Ethernet address.
- The only information that ARP possesses, at this point, is the IP address (say 192.168.0.1),
- so it basically sends a request to all stations on the local network, asking, "Who has the IP address 192.168.0.1?"
- The receiving station that has been assigned the relevant IP address responds with its own Ethernet address.

ARP conversation



RARP conversation



ICMP: Internet Control Message Protocol

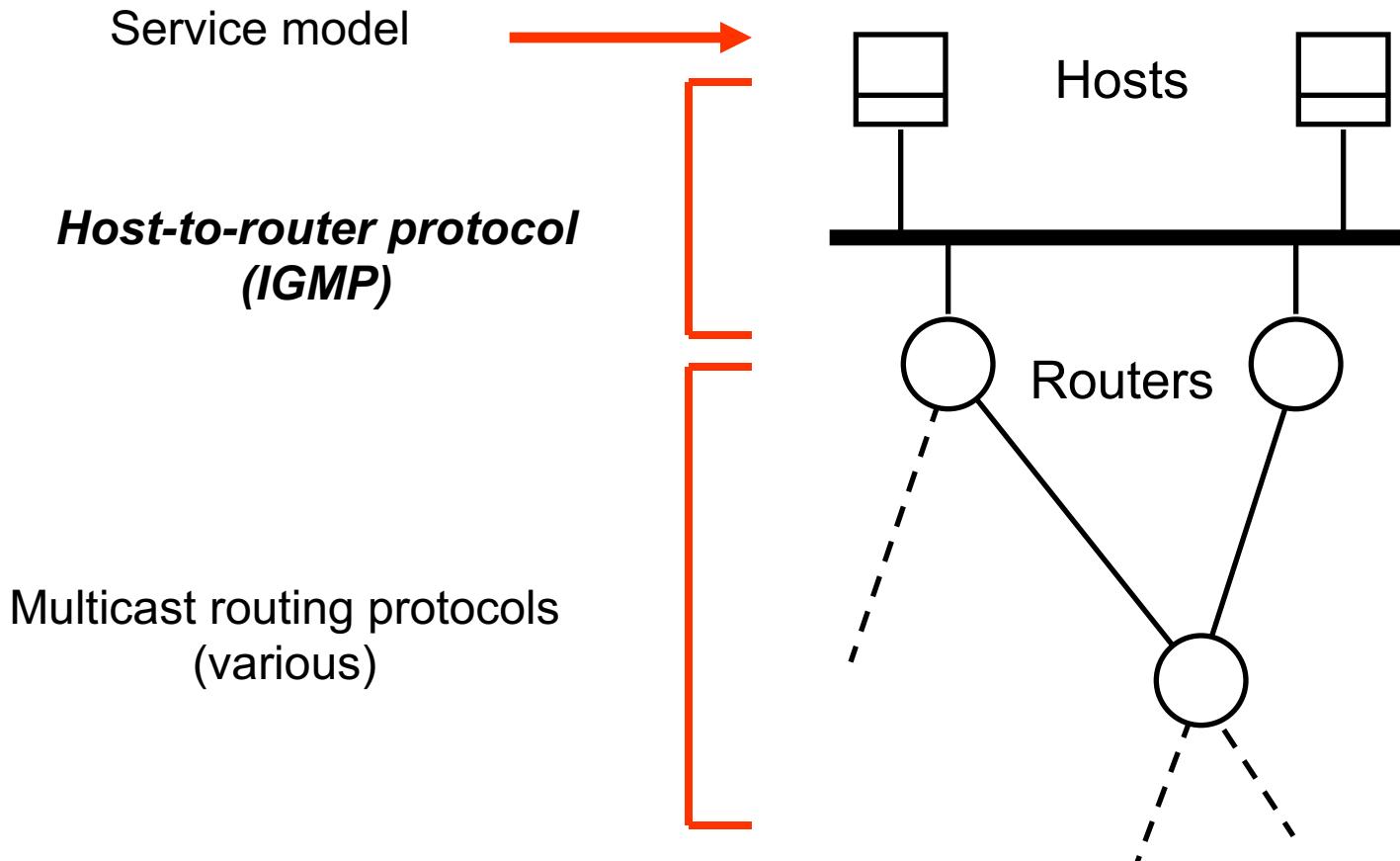
- ICMP is a protocol used for exchanging control messages.
- ICMP uses IP to deliver messages.
- ICMP messages are usually generated and processed by the IP software, not the user process.

ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

ICMP messages are divided into error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter. The query messages get specific information from a router or another host.

Internet Group Management Protocol (IGMP)



IGMP

- End system to router protocol is IGMP
- Each host keeps track of which multicast groups are subscribed to
 - Socket API informs IGMP process of all joins
- Objective is to keep router up-to-date with group membership of entire LAN
 - Routers need not know who all the members are, only that members exist

Transport Layer

- Sequencing and transmitting of packets
- Acknowledgment of receipts
- Recovery of packets
- Flow control
- In essence, it engages in host-to-host transportation of data packets and the delivery of them to the application layer
- Functionality of transport layer
 - Support arbitrary message size at the application level
 - Support in-order delivery of messages
 - Shield the application from loss of messages
 - Shield the application from bit errors in transmission.

Core Protocols of the Transport Layer

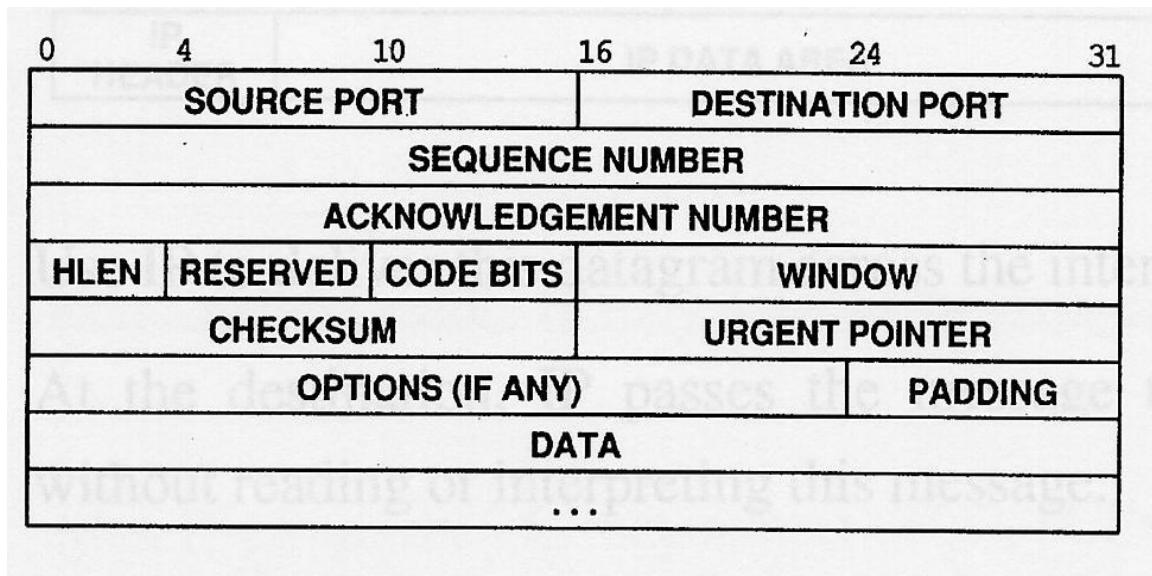
TCP
(Transmission
Control Protocol)

UDP (User
Datagram Protocol)

Transport Layer

TCP: Transmission Control Protocol

- TCP is an alternative transport layer protocol supported by TCP/IP.
- TCP provides:
 - Connection-oriented
 - Reliable
 - Full-duplex
 - Byte-Stream



Basic features of TCP

- TCP provides connection-oriented communication (virtual circuit connection, like telephone communication).
- It manages a point-to-point and full-duplex connection for an application between two computers as :
 - creates a connection before communication;
 - sends and receives data over this connection;
 - Application data is considered to be a continuous unstructured stream of bits.
 - Application programs must understand stream contents and boundaries of records.
 - closes a connection after communication.
- TCP guarantees reliable data delivery.
- The TCP recipient will receive data in a correct order without data loss or error.

User Datagram Protocol

- UDP is a transport-layer protocol
 - communication between processes
- UDP uses port to deliver datagrams to the right host.
- Used in video and audio casting
 - Multicasting
 - Broadcasting
 - multimedia transmission

Basic properties of UDP

- **UDP is a connectionless transport protocol.**
 - A UDP application sends messages without establishing and closing a connection.
 - UDP has a smaller overhead than TCP, especially when the total size of the messages is small.
- **UDP does not guarantee reliable data delivery.**
 - UDP messages can be lost or duplicated, or they may arrive out of order; and they can arrive faster than the receiver can process them.
 - The application programmers using UDP have to consider and tackle these issues themselves.
- **UDP has no mechanism for flow control.**
- **Difference between UDP and IP**
 - UDP distinguishes among applications within a given host via the destination port number; an IP datagram only identifies a destination host via the IP address.

UDP

- Datagram Delivery
- Connectionless
- Unreliable
- Minimal

- The header consists of 8 bytes.
- The data can have a variable size.

UDP Datagram Format

Source Port	Destination Port
Length	Checksum
Data	

Application Layer

- Provides applications with the ability to access the services of the other layers
- New protocols and services are always being developed in this category

Core Protocols

- HTTP
- FTP
- Telnet
- SMTP
- POP3
- IMAP
- DNS
- RIP
- SNMP etc.

Application Related Application Layer Protocols

- HTTP
- FTP
- SMTP
- Telnet

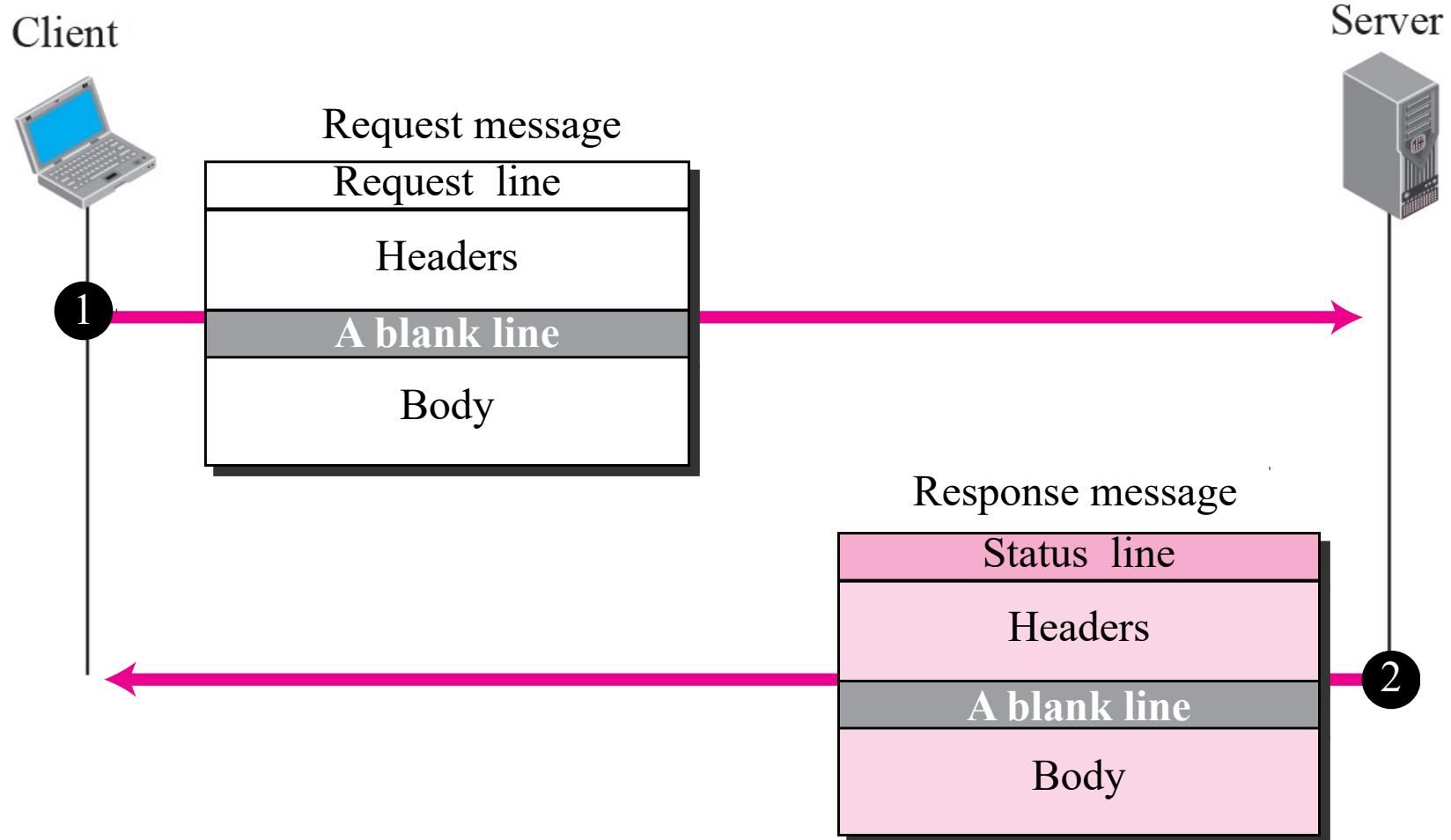
LAN Management/Operation Related Application Layer Protocols

- DNS
- RIP
- SNMP

Hyper Text Transfer Protocol (HTTP)

- Protocol relating to web applications
- Access data on the World Wide Web
- Functions like a combination of FTP and SMTP
- Similar to FTP because it transfers files and uses the services of TCP
- However, it is much simpler than FTP because it uses only one TCP connection
- Default port number is 80

HTTP transaction

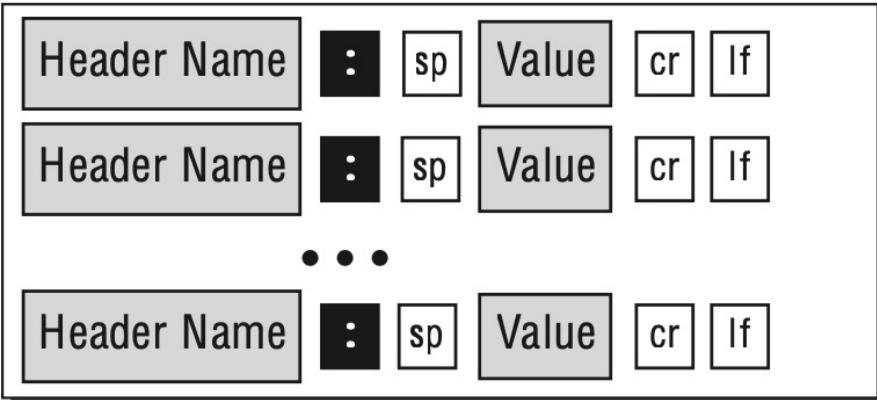


HTTP transaction

Request Line



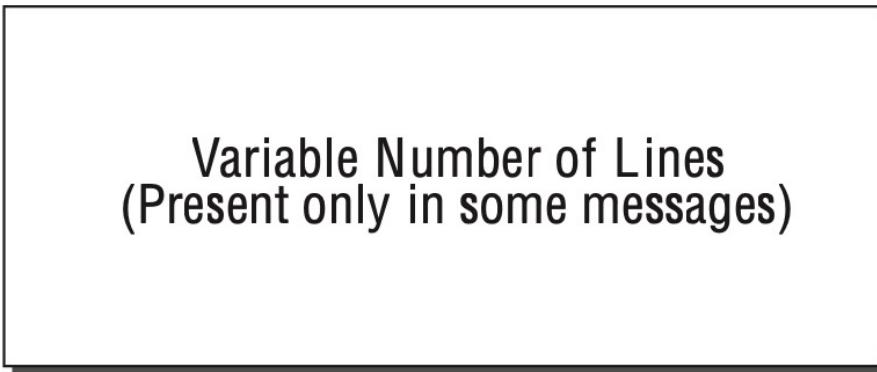
Header Lines



Blank Line



Body



Legend

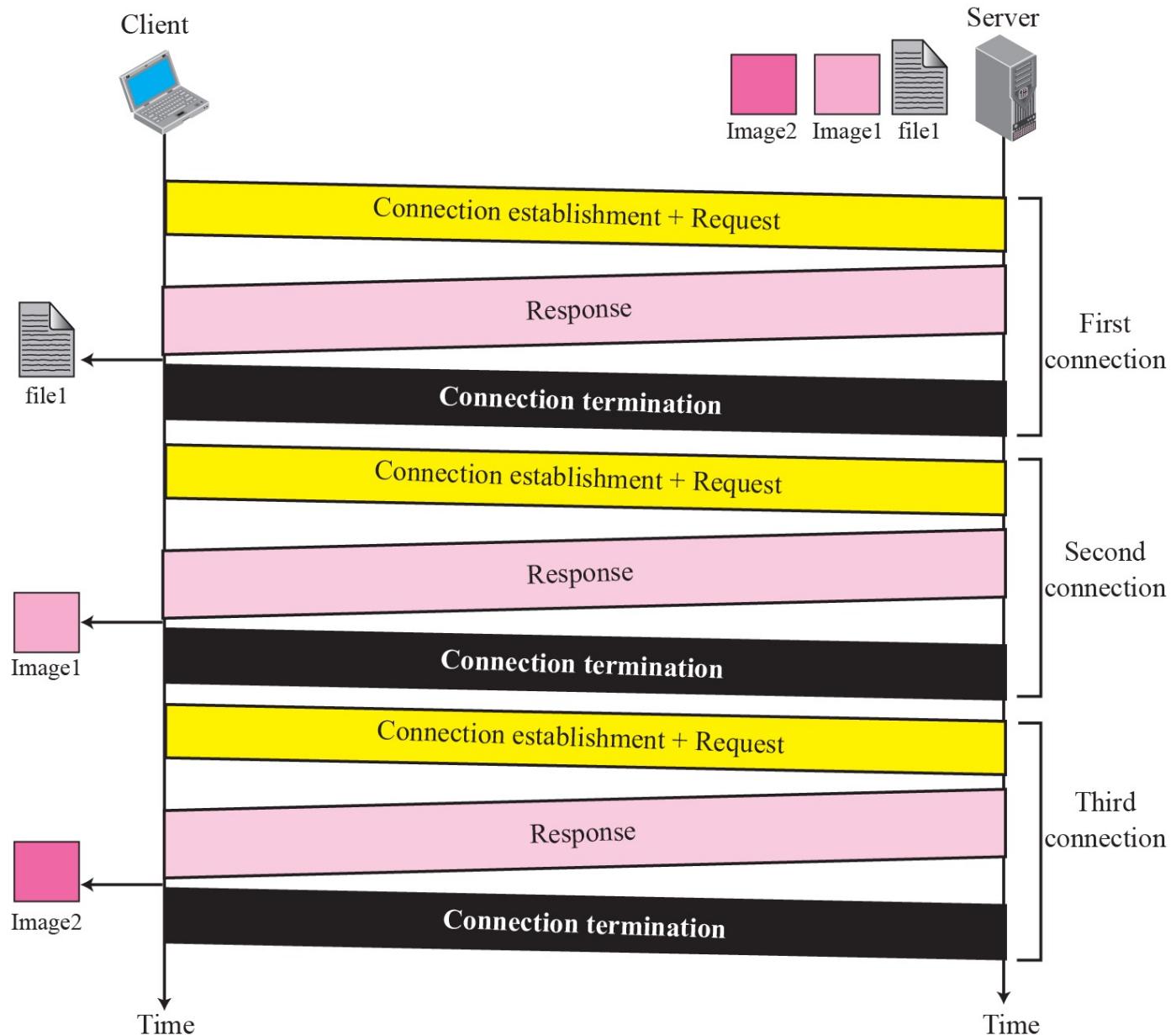
sp: Space
cr: Carriage Return
lf: Line Feed

HTTP transaction

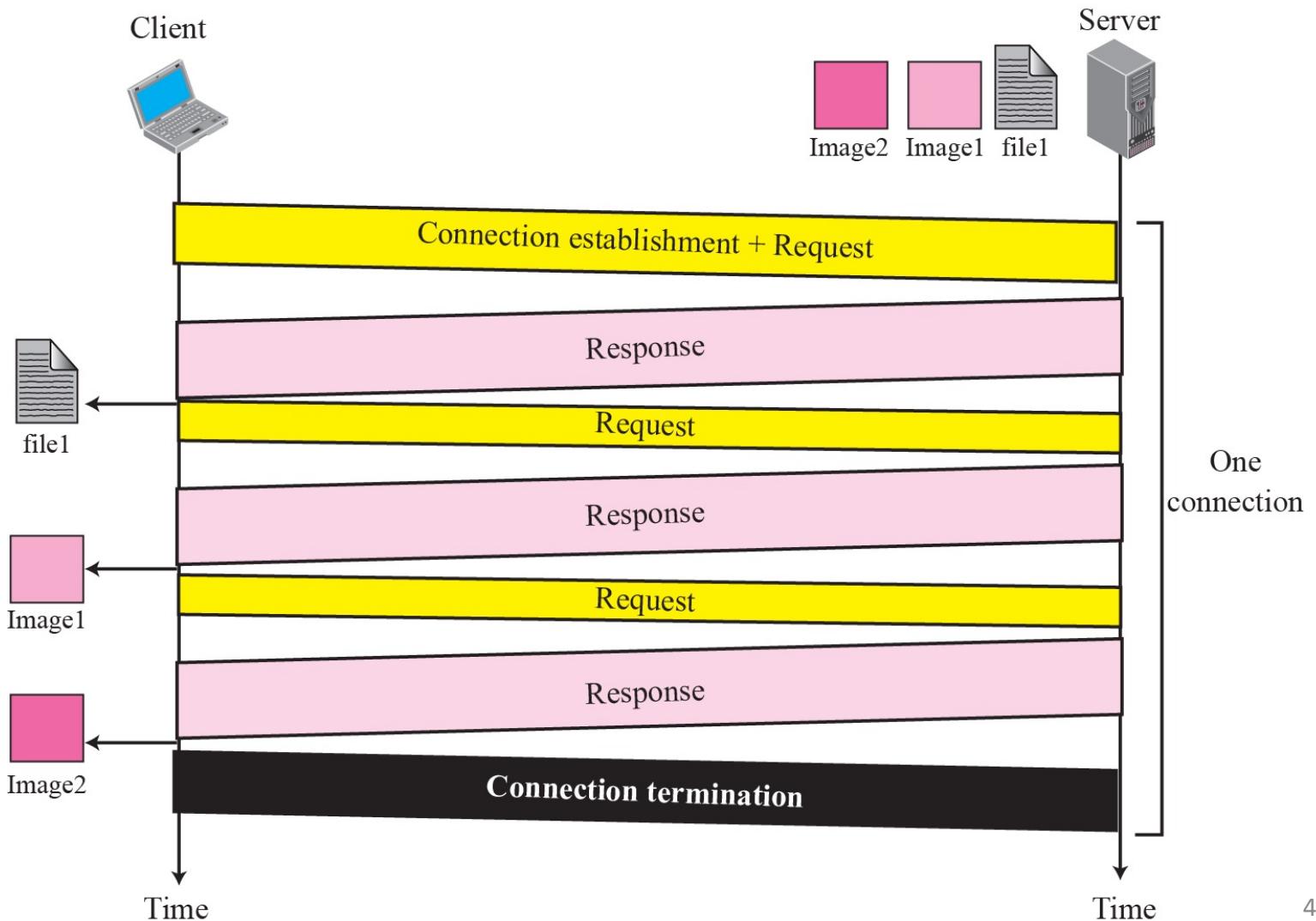
Table 22.1 *Methods*

<i>Method</i>	<i>Action</i>
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
DELETE	Remove the Web page
OPTIONS	Enquires about available options

Non-Persistent HTTP connection



Persistent HTTP connection



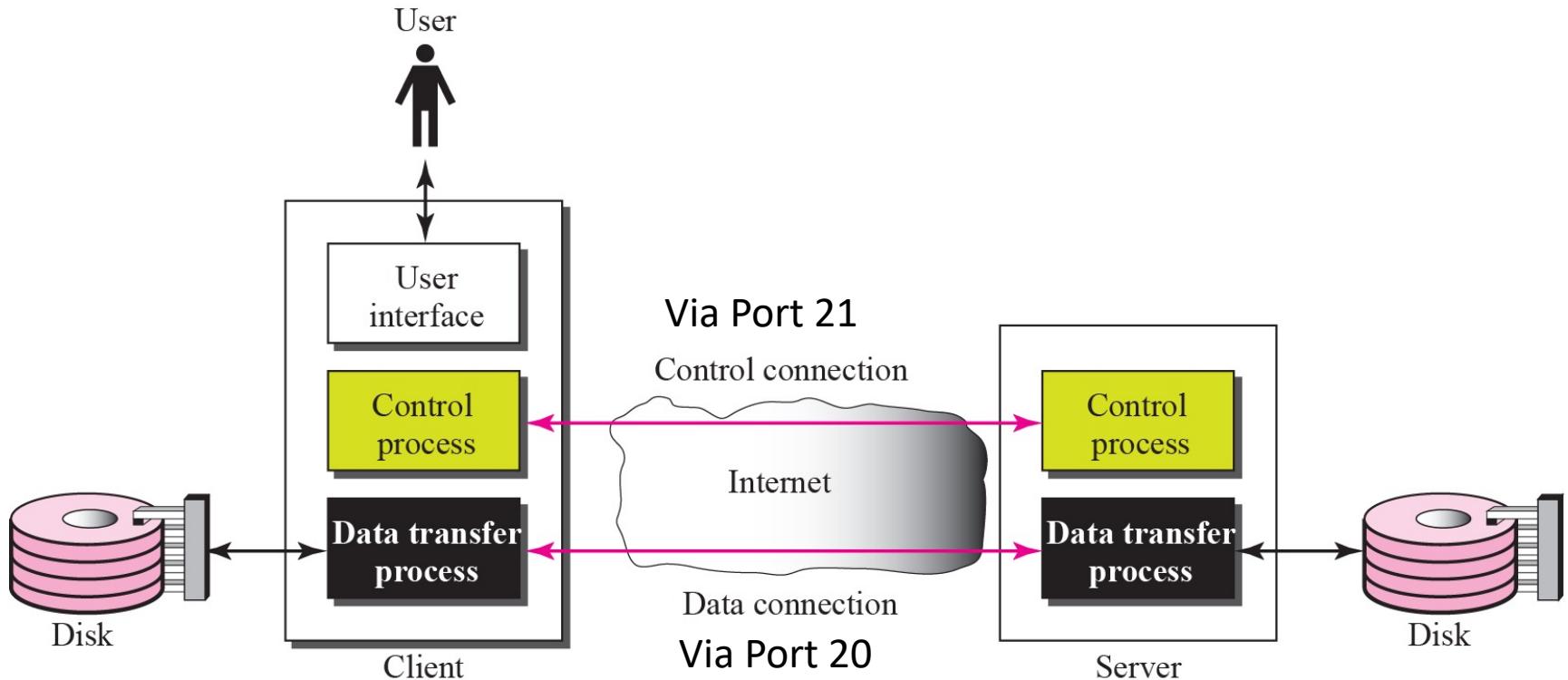
File Transfer Protocol (FTP)

- Standard mechanism for copying a file from one host to another
- Designed for faster file transfer over the Internet compared to using the HTTP protocol
- FTP sites can be configured alongside a web site to support FTP file transfer
- FTP default ports are 20 and 21

Note

*FTP uses the services of TCP.
It needs two TCP connections. The well-known port 21 is used for the control connection and the well-known port 20 for the data connection.*

FTP



FTP

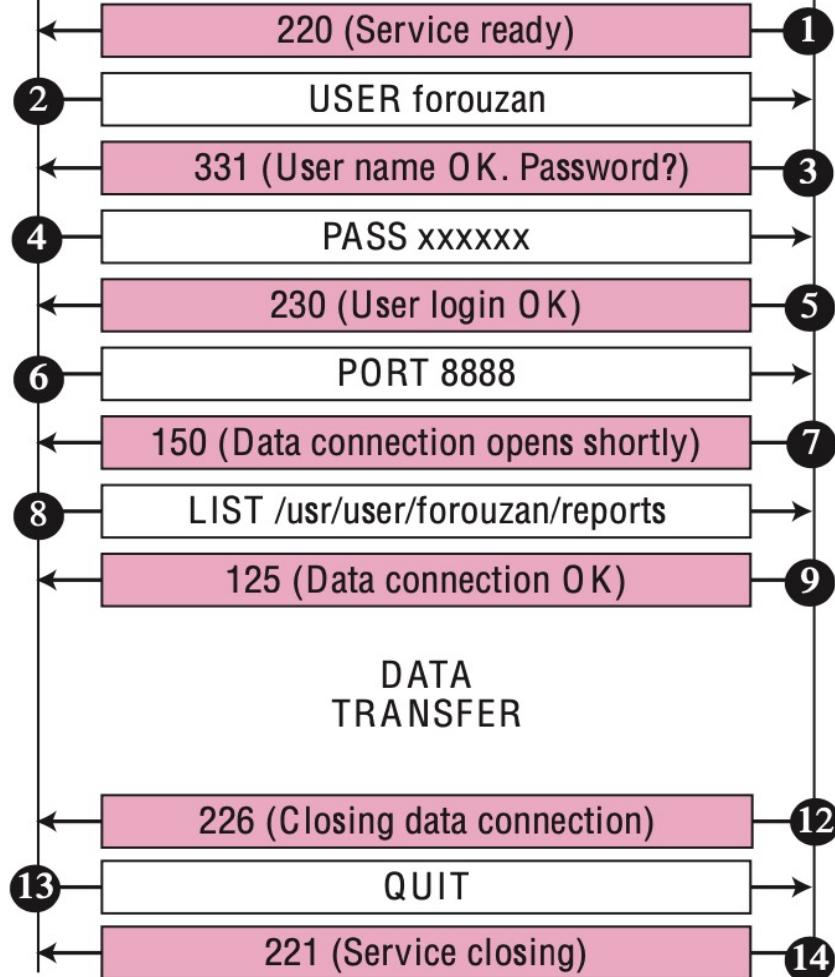
Client

Server

Control process

Control connection

Control process



Client

Data process

Data connection

Server

Data process

List of files or directories

10

List of files or directories

11

FTP

<i>Code</i>	<i>Description</i>
Transient Negative Completion Reply	
425	Cannot open data connection
426	Connection closed; transfer aborted
450	File action not taken; file not available
451	Action aborted; local error
452	Action aborted; insufficient storage
Permanent Negative Completion Reply	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command parameter not implemented
530	User not logged in
532	Need account for storing file
550	Action is not done; file unavailable
552	Requested action aborted; exceeded storage allocation
553	Requested action not taken; file name not allowed

<i>Code</i>	<i>Description</i>
Positive Preliminary Reply	
120	Service will be ready shortly
125	Data connection open; data transfer will start shortly
150	File status is OK; data connection will be open shortly
Positive Completion Reply	
200	Command OK
211	System status or help reply
212	Directory status
213	File status
214	Help message
215	Naming the system type (operating system)
220	Service ready
221	Service closing
225	Data connection open
226	Closing data connection
227	Entering passive mode; server sends its IP address and port number
230	User login OK
250	Request file action OK
Positive Intermediate Reply	
331	User name OK; password is needed
332	Need account for logging
350	The file action is pending; more information needed

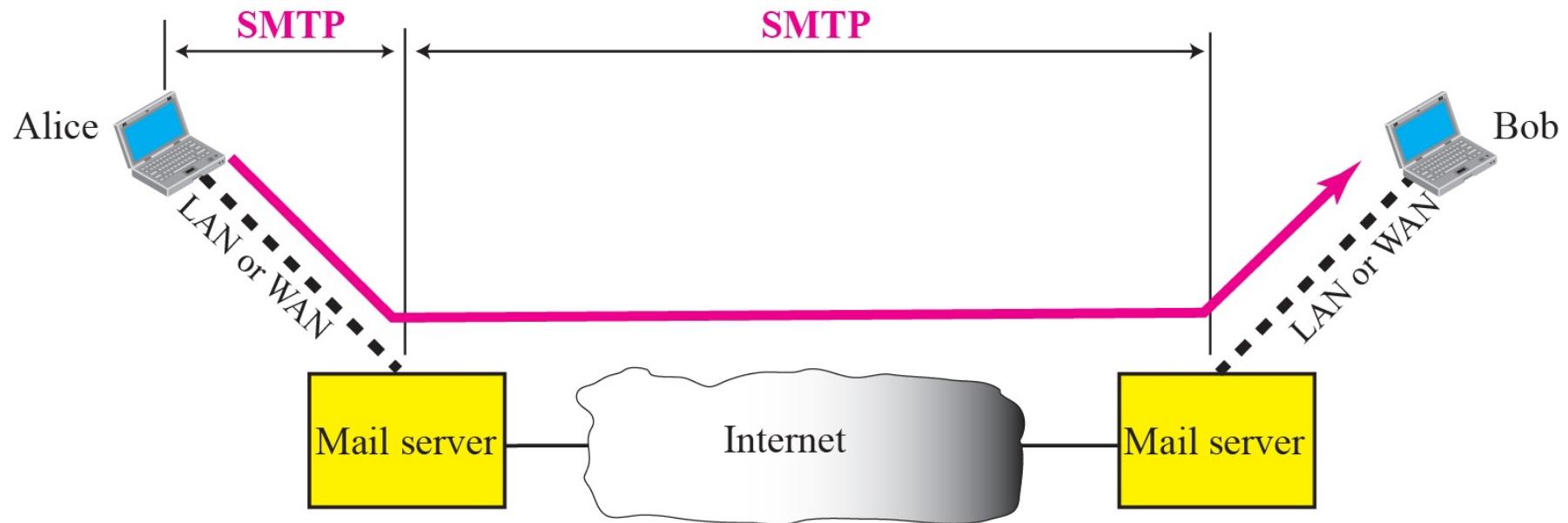
HTTP and FTP

- File transfer under FTP is faster than file transfer under HTTP
- Choose an FTP site if there is one for downloading files etc.

Simple Mail Transfer Protocol (SMTP)

- Governs the transmission of mail messages and attachments
- SMTP is used in the case of outgoing messages
- More powerful protocols such as POP3 and IMAP4 are needed and available to manage incoming messages

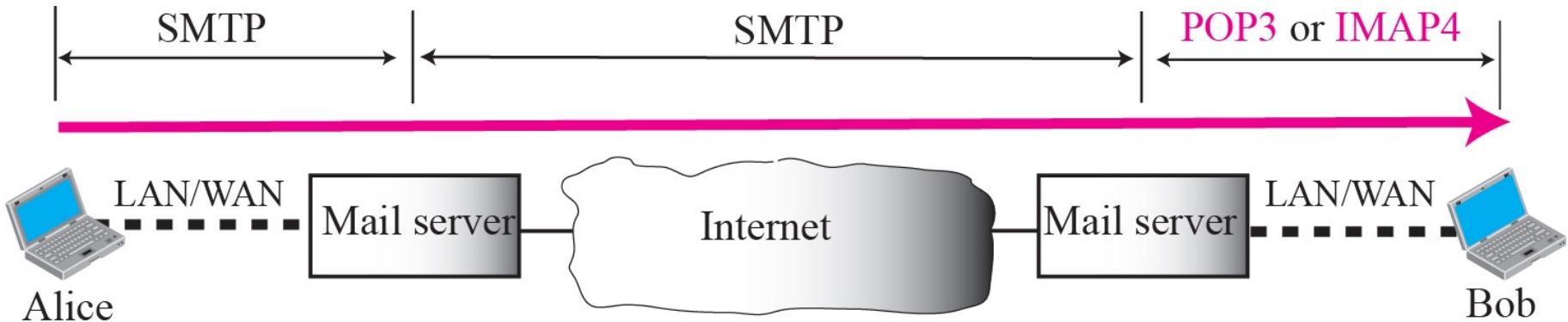
SMTP



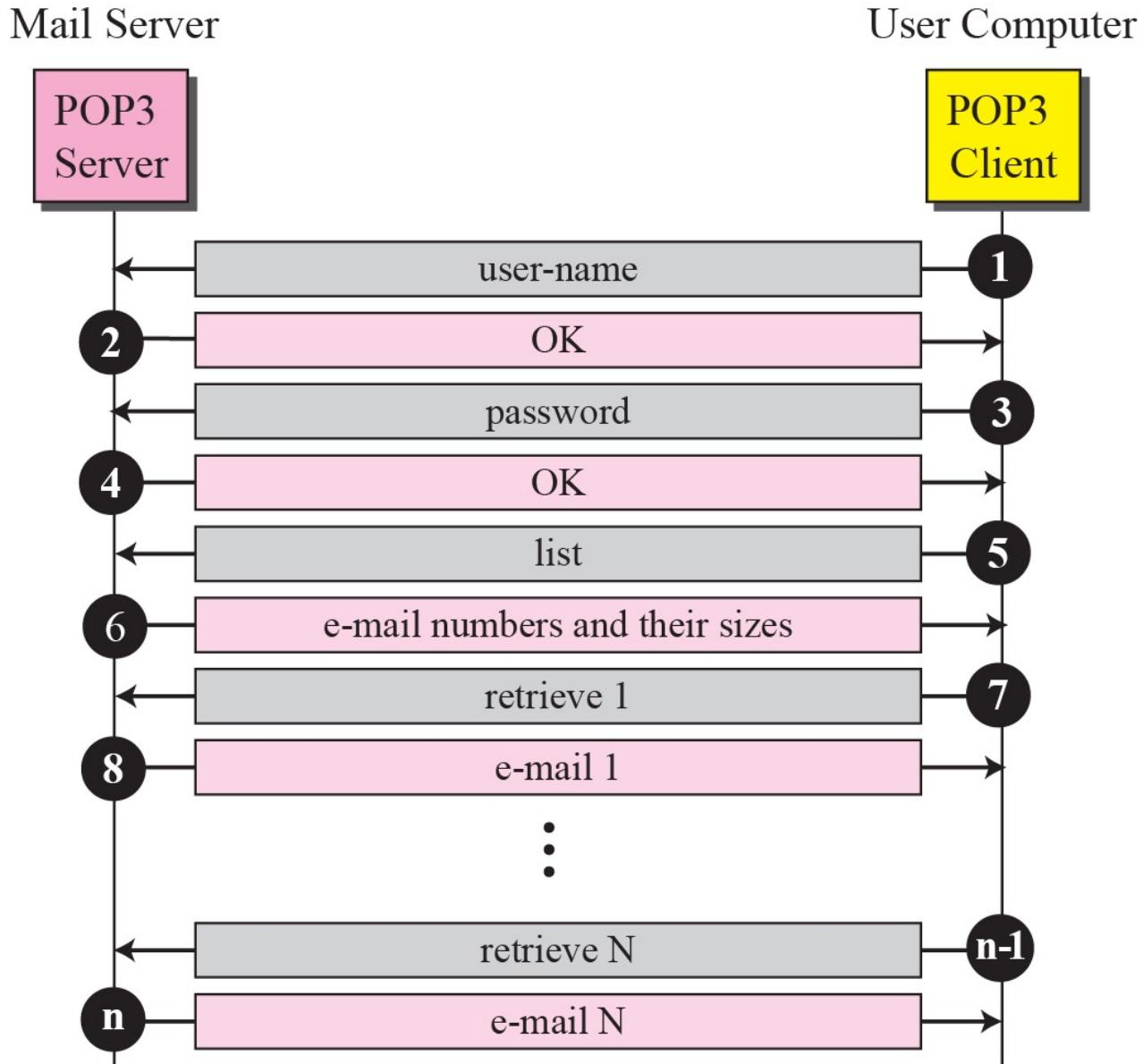
POP3/IMAP4

- Used for incoming mail
- POP3 is the older protocol
- IMAP4 is the more advanced protocol
- POP3 downloads the email from a server to a single computer, then deletes the email from the server.
- On the other hand, IMAP stores the message on a server and synchronizes the message across multiple devices.

Pop3 and IMAP4



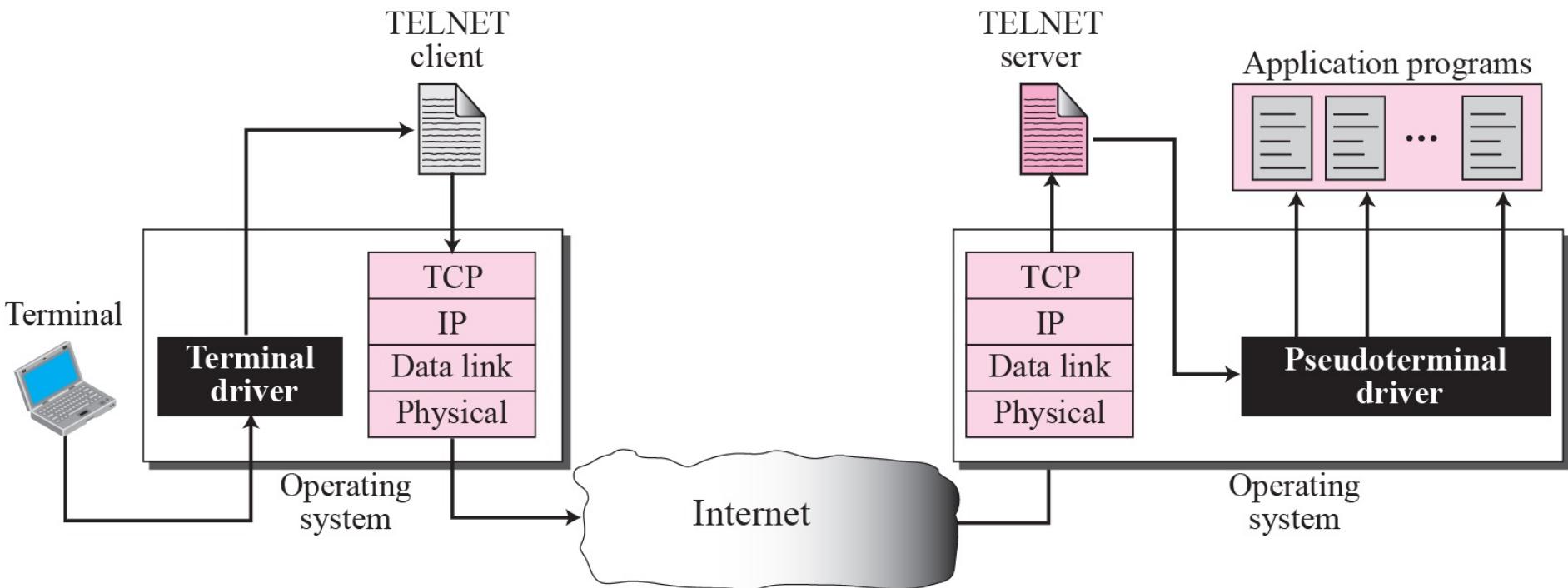
Post Office Protocol v3



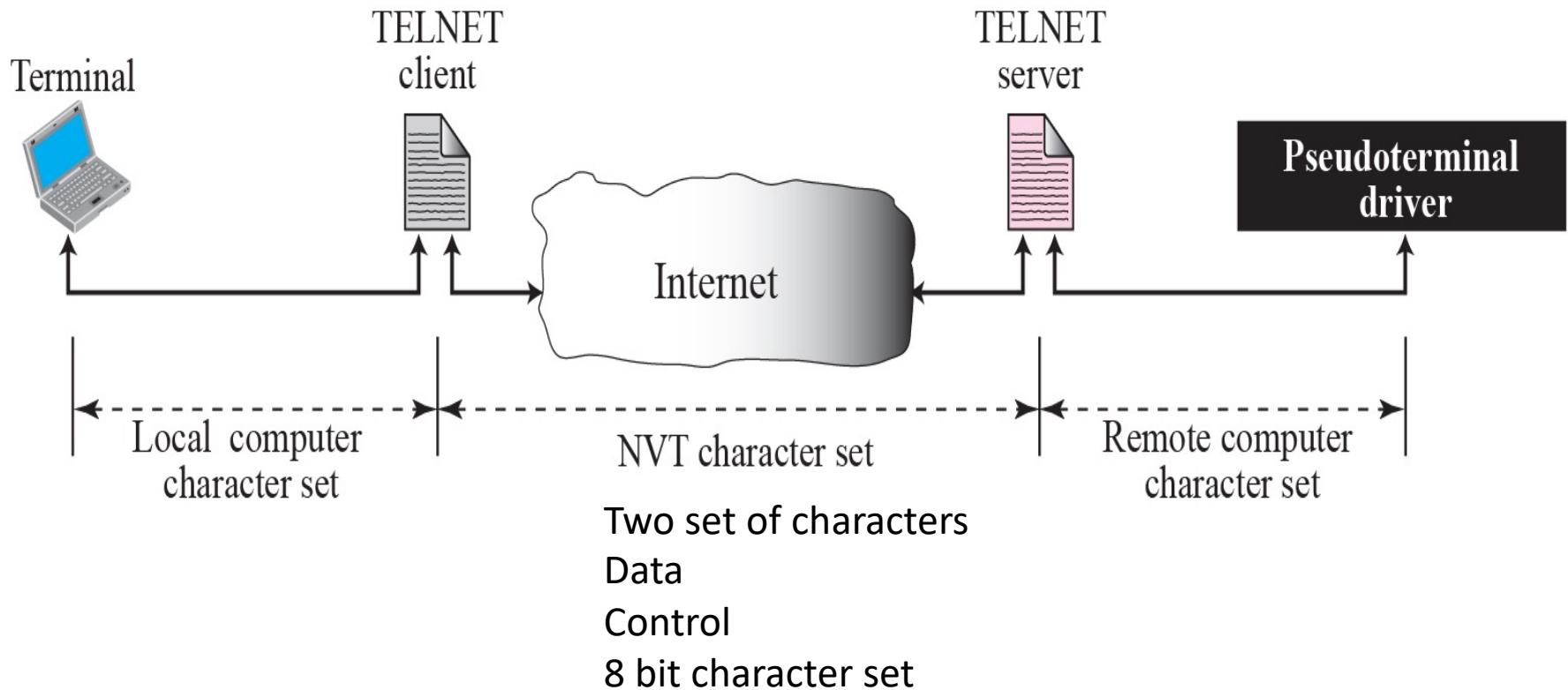
Telnet

- TELNET is for for TErminaL NETwork.
- Standard for TCP/IP protocol for virtual terminal service as proposed by ISO.
- TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.
- Used for accessing a Unix machine and emulating a terminal attached to the Unix computer

Remote login via TELNET



Network Virtual Terminal (NVT)

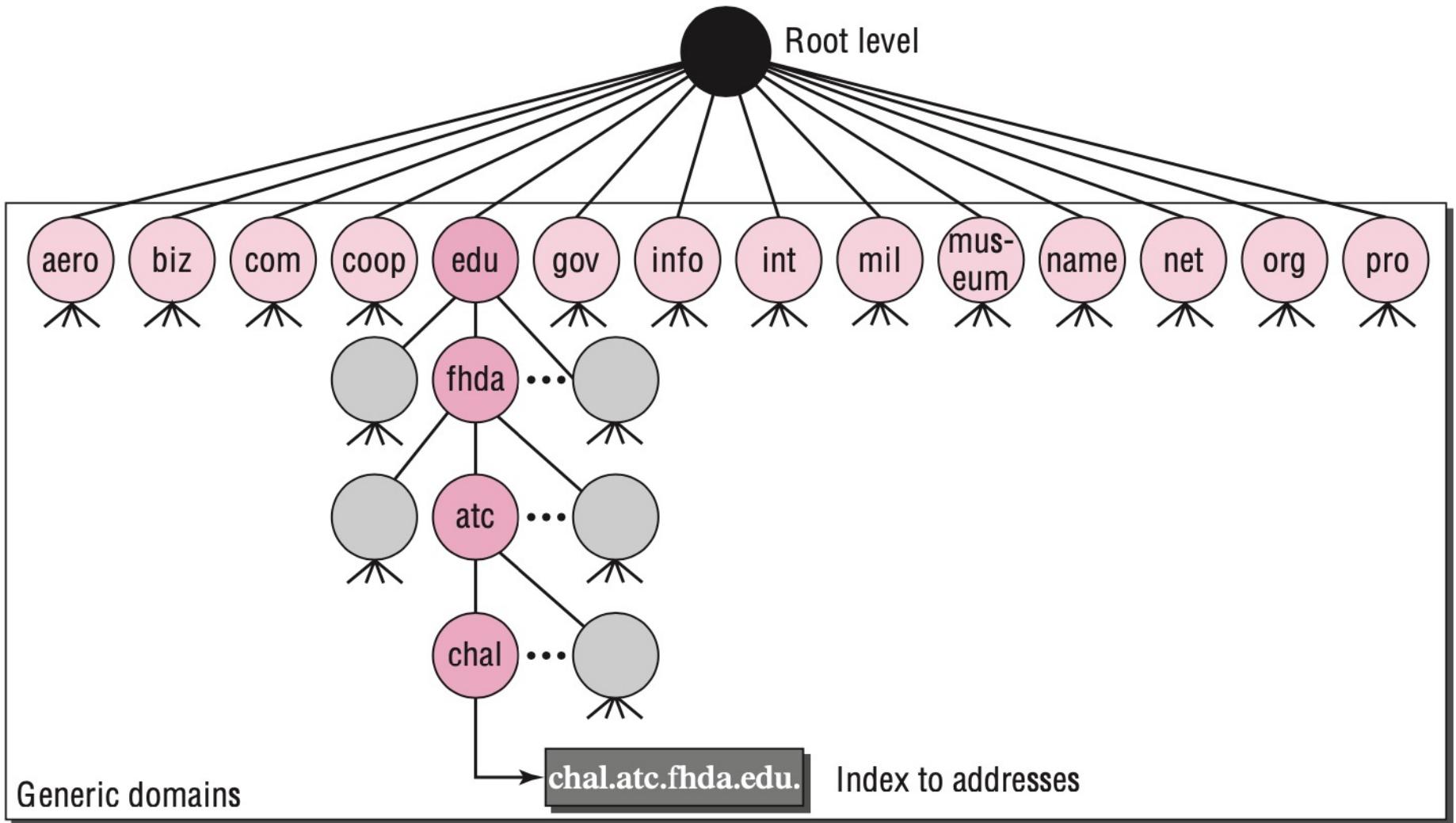


Domain Name System (DNS)

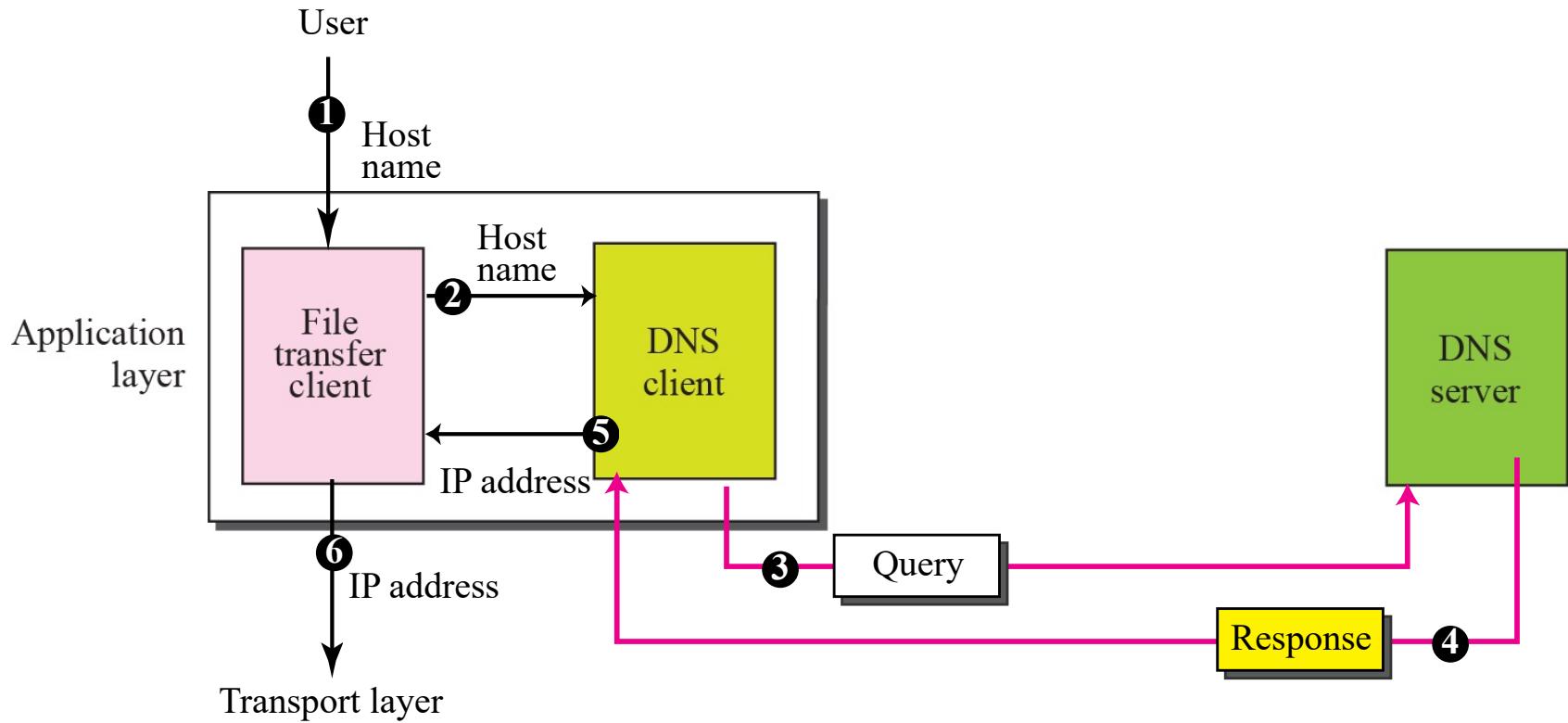
Resolves domain names to IP addresses
and vice versa



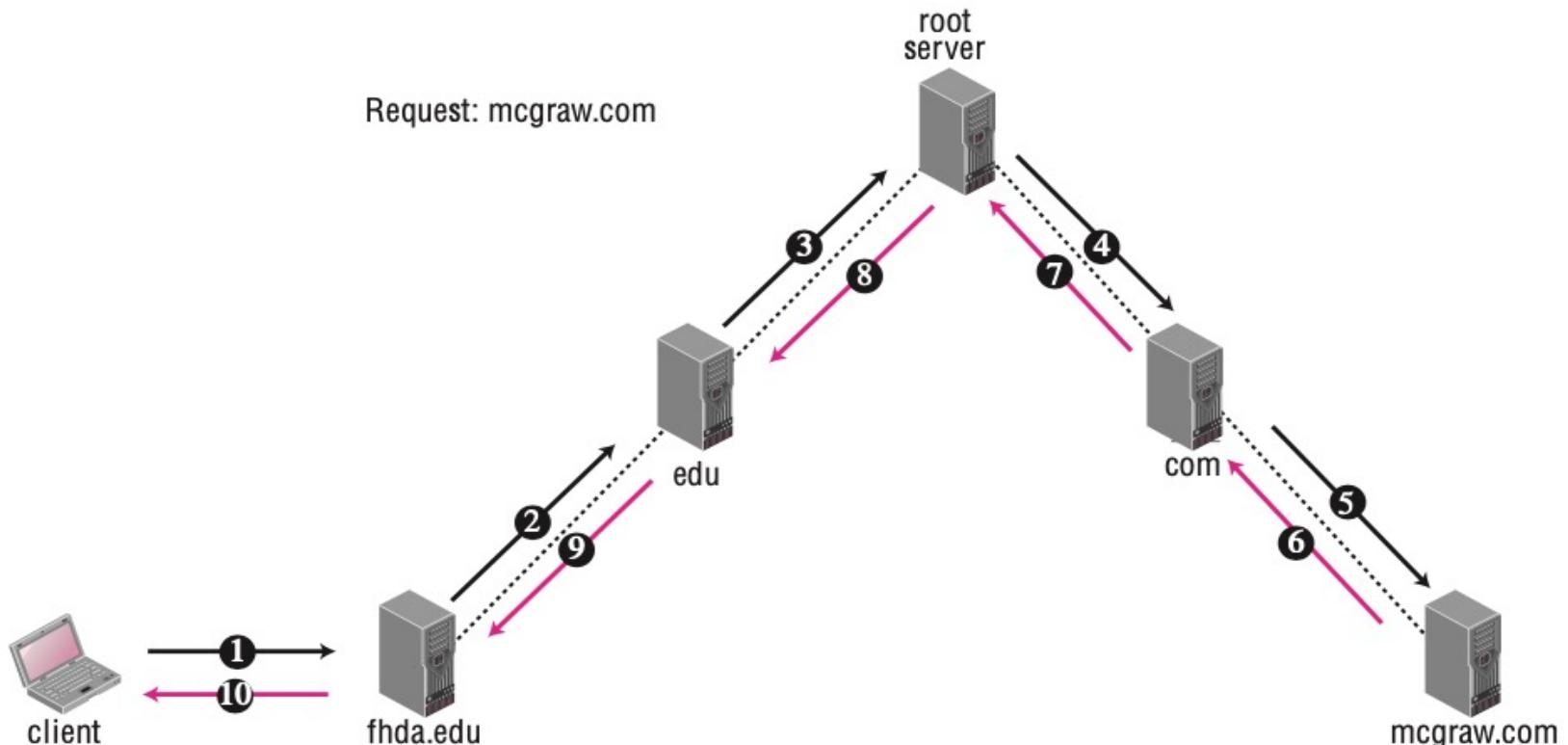
DNS



DNS

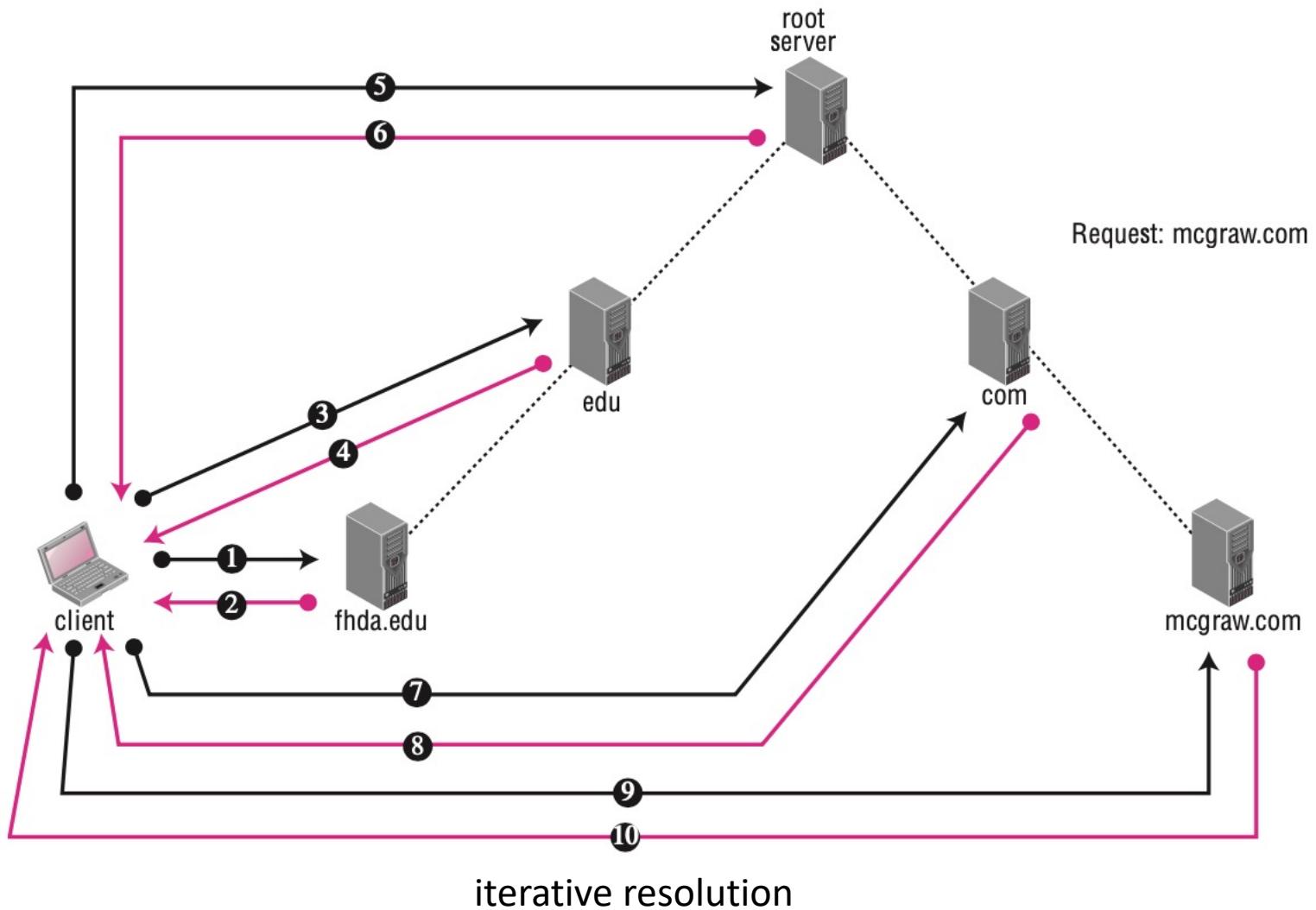


DNS address resolution

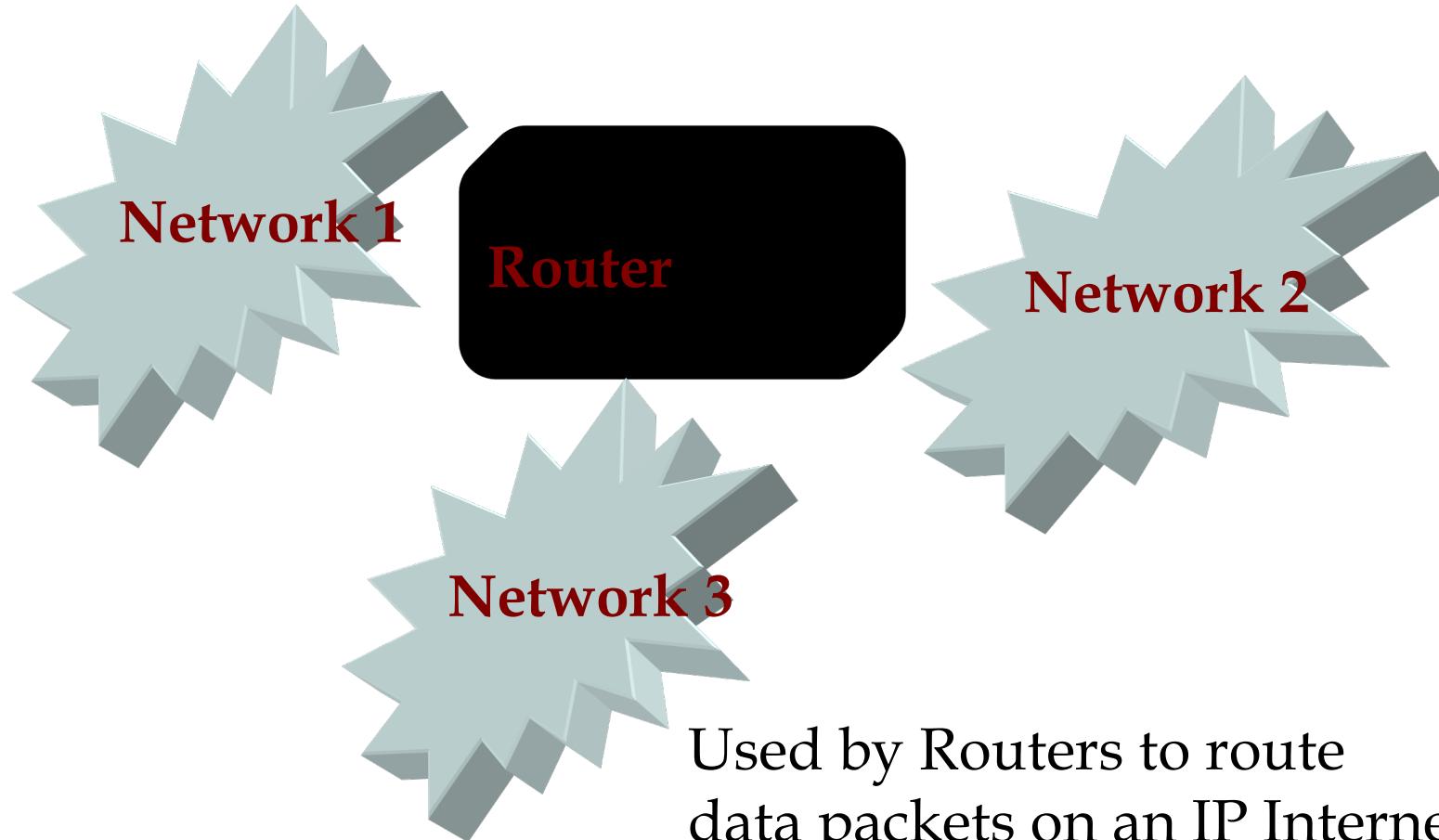


Recursive resolution

DNS address resolution



Routing Information Protocol (RIP)



RIP

- Intra-domain (interior) routing protocol used inside an autonomous system.
- Simple protocol based on distance vector routing.
- Implements distance vector routing directly with some considerations.

RIP messages

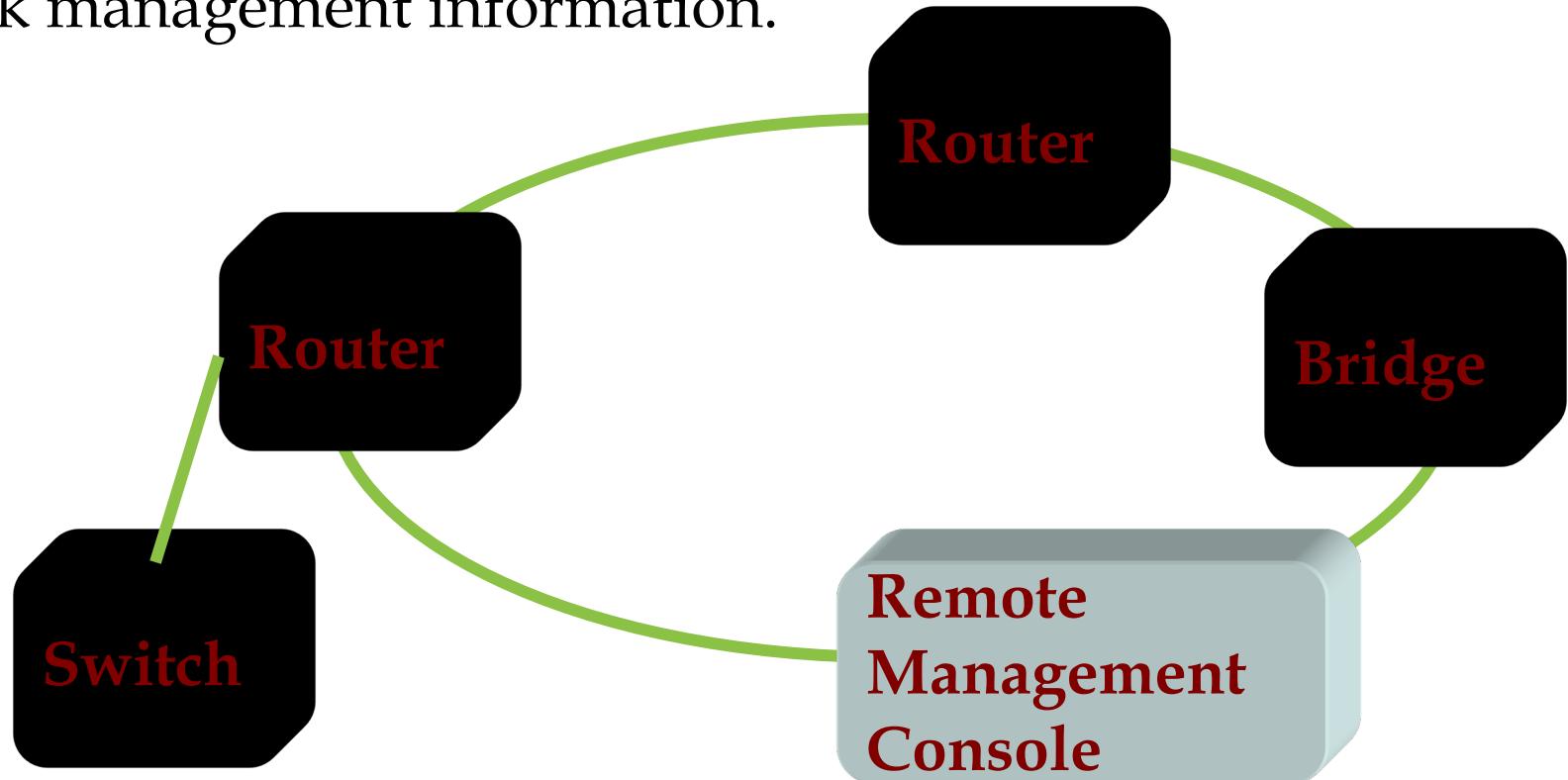
- Request
 - A request message is sent by a router that has just come up or by a router that has some time-out entries
 - A request can ask about specific entries or all entries
- Response
 - A response can be either solicited or unsolicited (30s or when there is a change in the routing table)

RIP Timers

- Periodic timer
 - It controls the advertising of regular update message (25 ~ 30 sec)
- Expiration timer
 - It governs the validity of a route (180 sec)
 - The route is considered expired and the hop count of the route is set to 16
- Garbage collection timer
 - An invalid route is not purged from the routing table until this timer expires (120 sec)

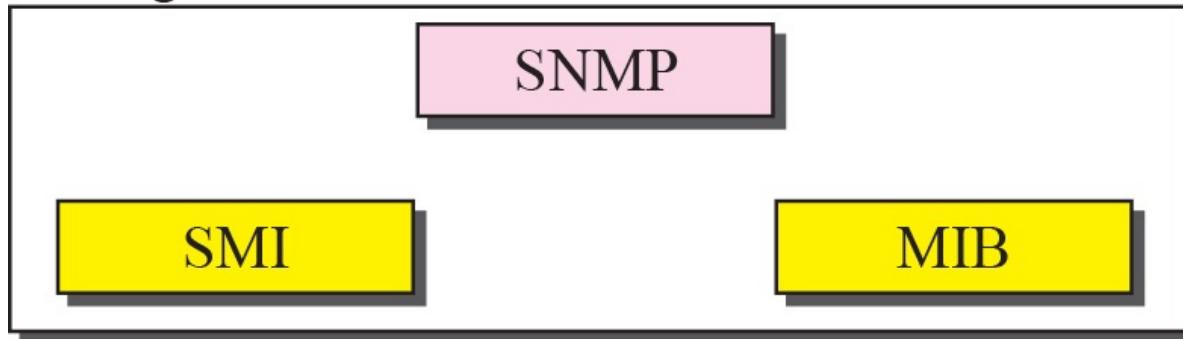
Simple Network Management Protocol (SNMP)

Facilitates the management of SNMP compliant routers, bridges, switches etc. by enabling the collection and exchange of network management information.



Network Management on the Internet

Management



- SNMP uses two other protocols for network management :
 - Structure of Management Information (SMI) and
 - Management Information Base (MIB).

Note

SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status of objects (values of variables) in SNMP packets.

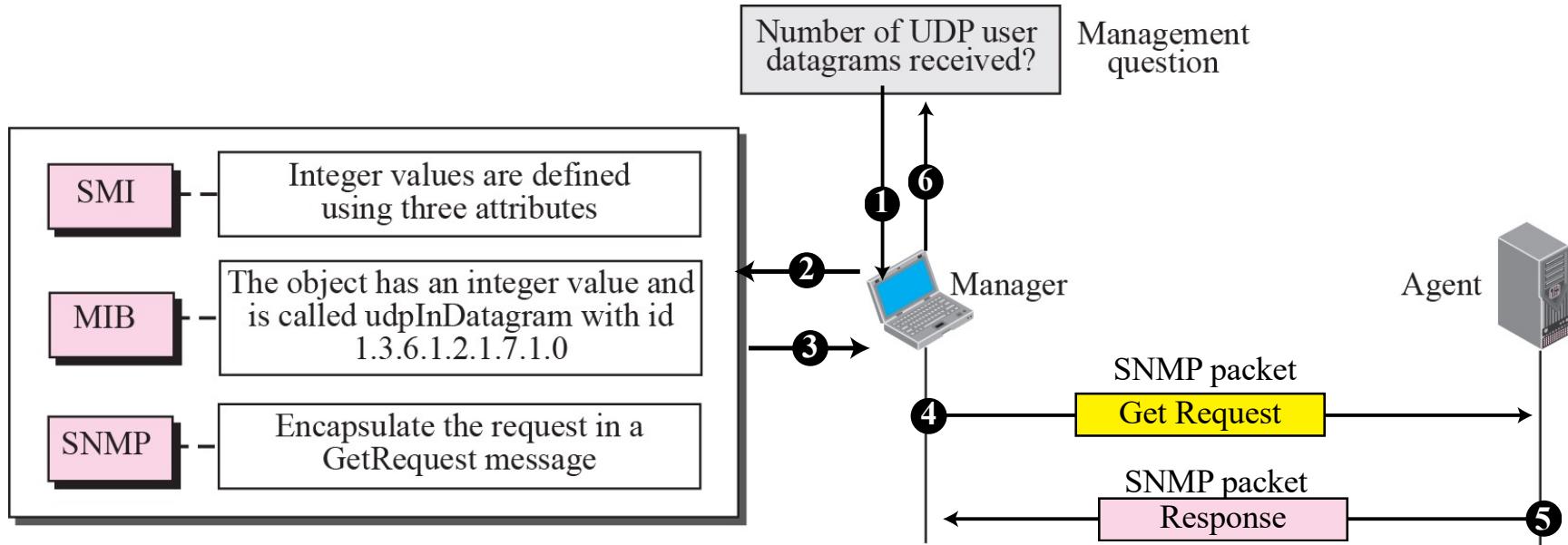
Note

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

Note

MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

Network Management overview



Thank You