Computer Networks
UNIT V

The Application Layer

Overview: The Application Layer

- Domain name system (DNS)
- Simple Network Management Protocol (SNMP)
- Electronic Mail
- The World WEB
- HTTP
- Streaming audio and video.

DNS- The Domain Name System

- DNS is hierarchical, domain-based naming scheme and a distributed database system for implementing the naming scheme used in internet.
- It is primarily used for mapping host names and e-mail destinations to IP addresses.
- To map a name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter.

DNS- The Domain Name System

- The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller.
- Armed with the IP address, the program can then establish a TCP connection with the destination or send it UDP packets.

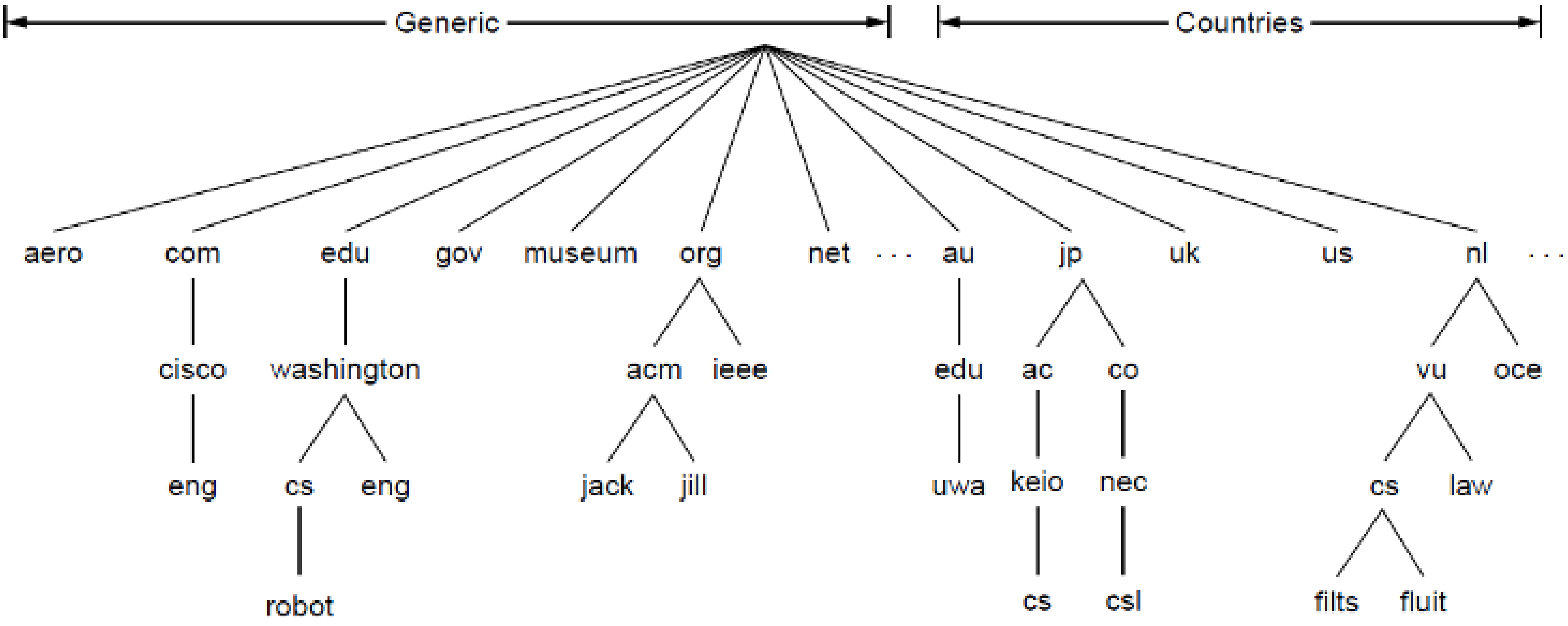
DNS- The Domain Name System

- Domain names can be either absolute or relative.
- An absolute domain name always ends with a period (e.g., eng.sun.com.), whereas a relative one does not.
- Relative names have to be interpreted in some context to uniquely determine their true meaning.
- In both cases, a named domain refers to a specific node in the tree and all the nodes under it.

DNS- The Domain Name System

- Domain names are case insensitive, Component names can be up to 63 characters long, and full path names must not exceed 255 characters.
- To create a new domain, permission is required of the domain in which it will be included.
- Naming follows organizational boundaries, not physical networks.

The DNS Name Space (1)

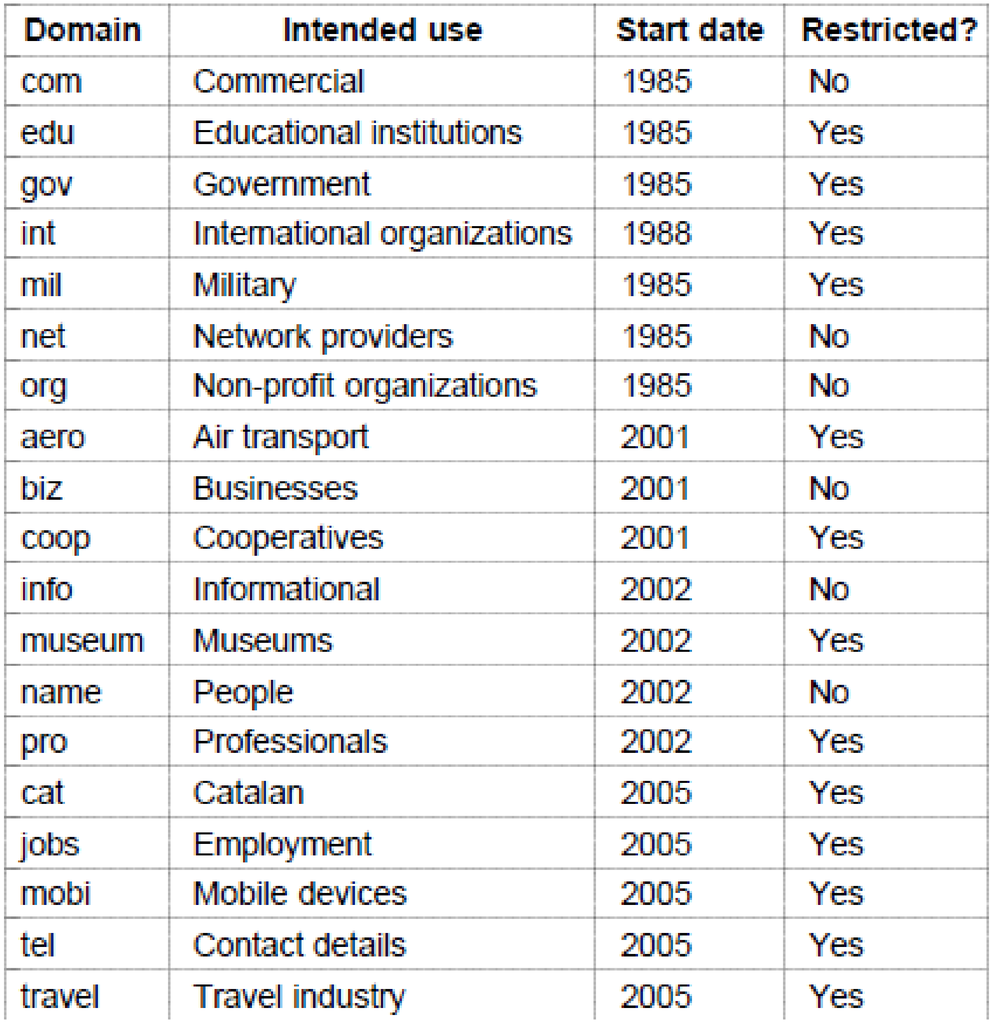


A portion of the Internet domain name space.

- The Internet is divided into over 200 top-level domains, where each domain covers many hosts.
- Each domain is partitioned into subdomains, and these are further partitioned, and so on.
- All these domains can be represented by a tree.

- The leaves of the tree represent domains that have no subdomains.
- A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.
- The top-level domains come in two flavors: generic and countries.
- Each domain is named by the path upward from it to the root.
- The components are separated by periods (pronounced ''dot'').

The DNS Name Space: Generic top-level domains



Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes

Resource records

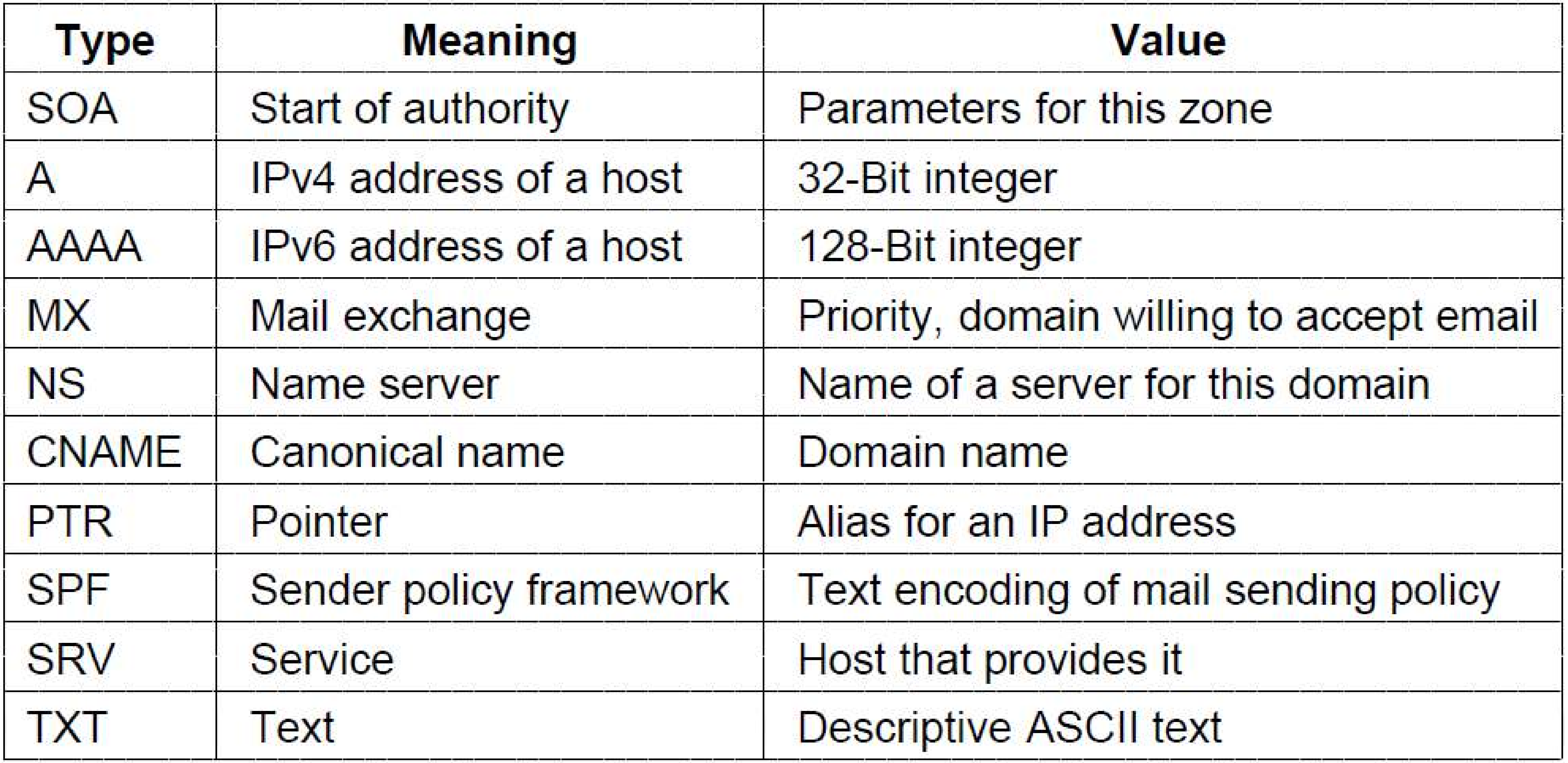
- Every domain has a set of resource records associated with it.
- When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name.
- Thus, the primary function of DNS is to map domain names onto resource records.
- A resource record is a five-tuple as follows:

Domain_name Time_to_live Class Type Value

Domain_name Time_to_live Class Type Value

- The Domain_name tells the domain to which this record applies.
- The Time_to_live field gives an indication of how stable the record is.
- The third field of every resource record is the Class.
  - For Internet information, it is always IN. For non-Internet information, other codes can be used.
- The Type field tells what kind of record this is.
- The Value field can be a number, a domain name, or an ASCII string.
  - The semantics depend on the record type.

Domain Resource Records



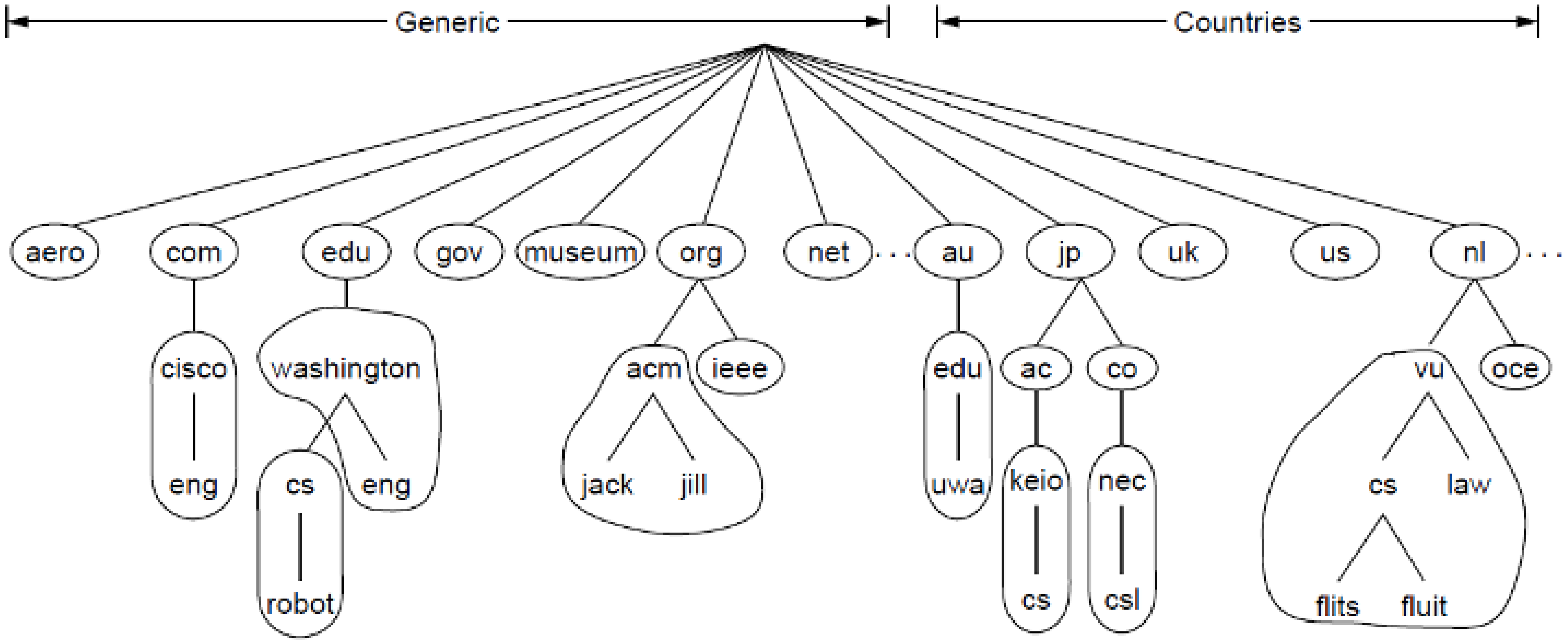
Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

The principal DNS resource record types

Name Servers

- To avoid the problems associated with having only a single source of information, the DNS name space is divided into nonoverlapping **zones**.
- Each zone contains some part of the tree and also contains name servers holding the information about that zone.
- Normally, a zone will have one primary name server, which gets its information from a file on its disk, and one or more secondary name servers, which get their information from the primary name server.

Name Servers



Part of the DNS name space divided into zones (which are circled).

Name Servers

- To improve reliability, some servers for a zone can be located outside the zone.
- Where the zone boundaries are placed within a zone is up to that zone's administrator.
- This decision is made in large part based on how many name servers are desired, and where.

- When a resolver has a query about a domain name, it passes the query to one of the local name servers.
- If the domain being sought falls under the jurisdiction of the name server, it returns the authoritative resource records.
- An **authoritative record** is one that comes from the authority that manages the record and is thus always correct.

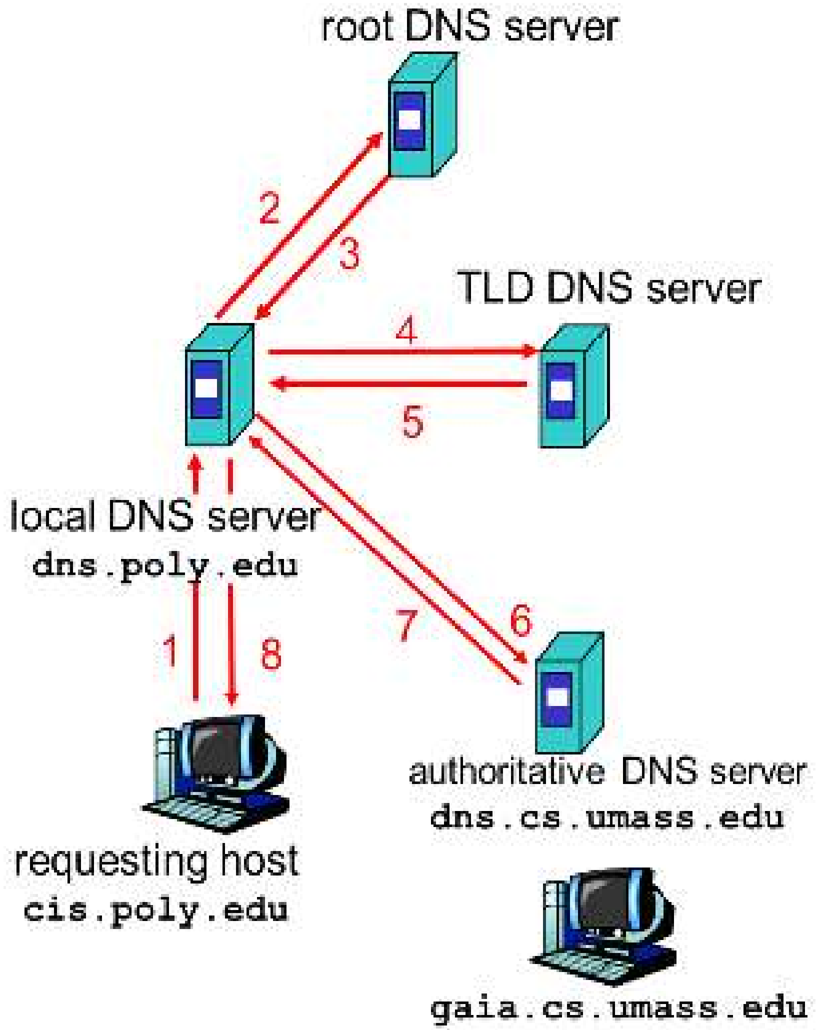
- Authoritative records are in contrast to cached records, which may be out of date.
- If, however, the domain is remote and no information about the requested domain is available locally, the name server sends a query message to the top-level name server for the domain requested using LDAP protocol.
- LDAP (Lightweight Directory Access Protocol) organizes information as a tree and allows searches on different components.

DNS Infrastructure & Resolution

Host at cis.poly.edu wants IP address for gaia.cs.umass.edu

Infrastructure:

- Client resolver
- Local DNS server
- Authoritative DNS Server
- Root DNS Server
- Top-Level Domain DNS Server



Simple Network Management Protocol SNMP

- What is SNMP?
- Basic SNMP components
- SNMP basic commands
- Typical SNMP communication
- SNMP versions (SNMP v1, v2 and v3)

What is SNMP?

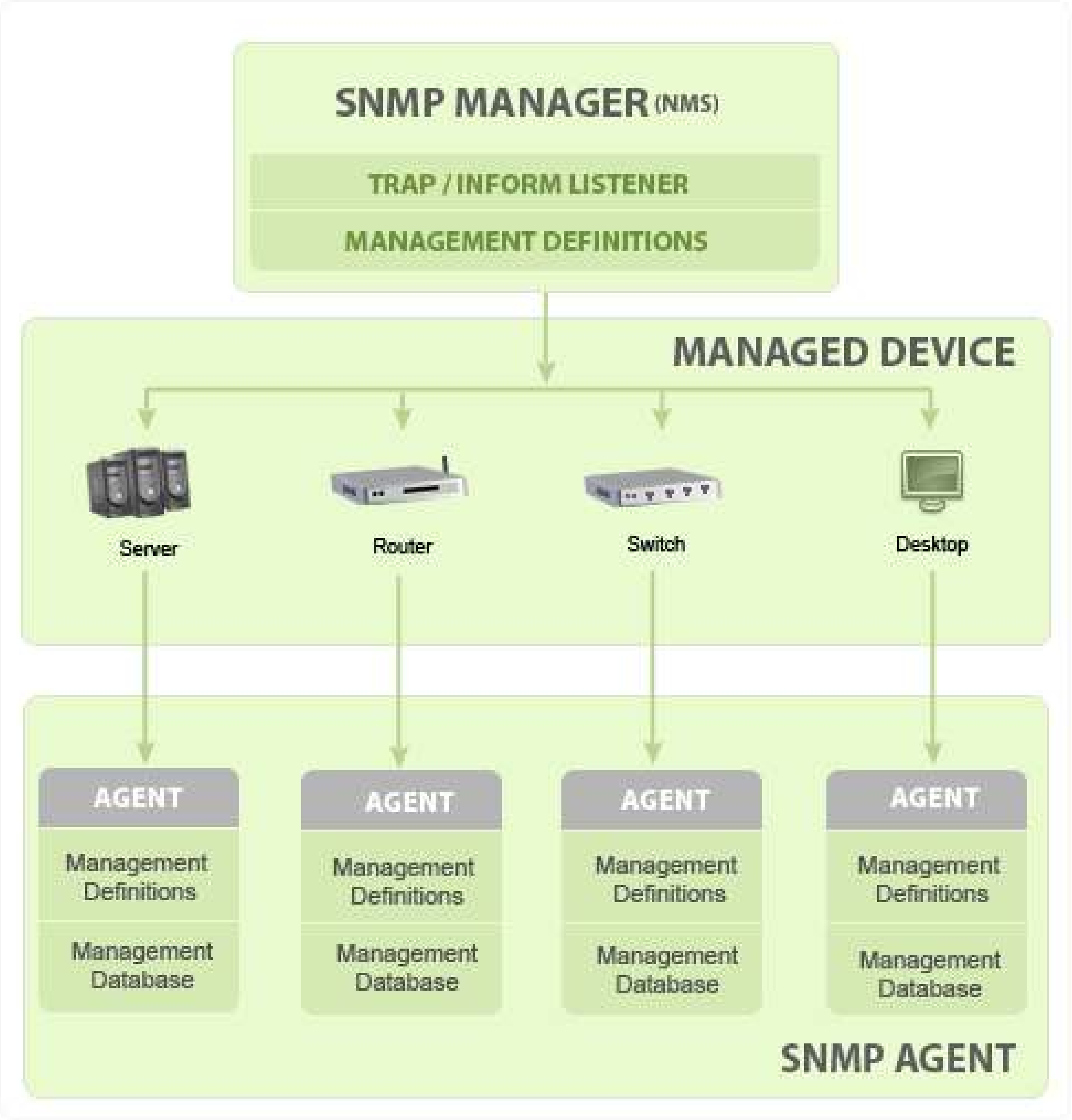
- Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices.
- It is a part of Transmission Control Protocol ⁄ Internet Protocol (TCP⁄IP) protocol suite.

- SNMP is one of the widely accepted network protocols to manage and monitor network elements.
- Most of the professional–grade network elements come with bundled SNMP agent.
- These agents have to be enabled and configured to communicate with the network monitoring tools or network management system (NMS).

SNMP basic components

- SNMP consists of
  - SNMP Manager
  - Managed devices
  - SNMP agent
  - Management Information Database (or Management Information Base - MIB)

SNMP Components



SNMP Manager:

- A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices.
- This is typically a computer that is used to run one or more network management systems.

- SNMP Manager’s key functions
  - Queries agents
  - Gets responses from agents
  - Sets variables in agents
  - Acknowledges asynchronous events from agents

Managed Devices:

- A managed device or the network element is a part of the network that requires some form of monitoring and management.
- managed devices include routers, switches, servers, workstations, printers, UPSs, etc...

SNMP Agent:

- The agent is a program that is packaged within the network element.
- Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for.
- These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

- SNMP agent’s key functions
  - Collects management information about its local environment
  - Stores and retrieves management information as defined in the MIB.
  - Signals an event to the manager.
  - Acts as a proxy for some non–SNMP manageable network node.

Management Information database or Management Information Base (MIB)

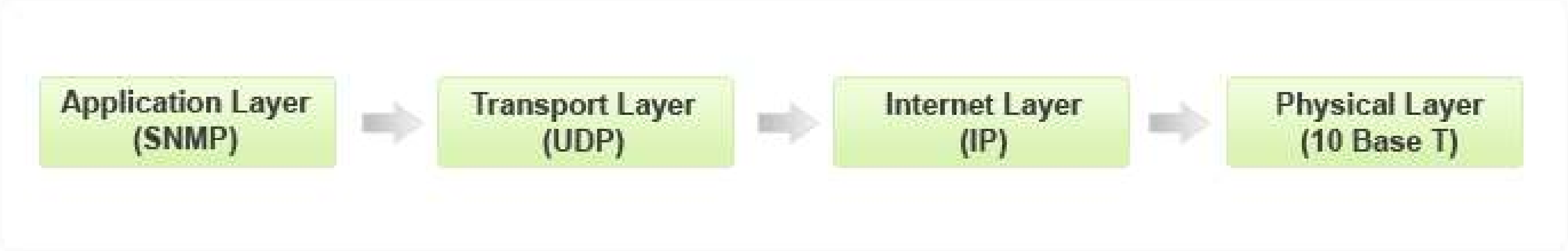
- Every SNMP agent maintains an information database describing the managed device parameters.
- The SNMP manager uses this database to request the agent for specific information.
- This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).
- In short,
  - MIB files are the set of questions that a SNMP Manager can ask the agent.
  - Agent collects these data locally and stores it, as defined in the MIB.
  - So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

Basic commands of SNMP

- The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands as given below
  - **GET**: The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.
  - **SET**: This operation is used by the managers to modify or assign the value of the Managed device.
  - **TRAPS**: Unlike the above commands which are initiated from the SNMP Manager, TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
  - **INFORM**: This command is similar to the TRAP initiated by the Agent, additionally INFORM includes confirmation from the SNMP manager on receiving the message.
  - **RESPONSE**: It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

Typical SNMP communication

- Being the part of TCP/ IP protocol suite, the SNMP messages are wrapped as User Datagram Protocol (UDP) and in turn wrapped and transmitted in the Internet Protocol.
- The following diagram illustrates the four–layer model.

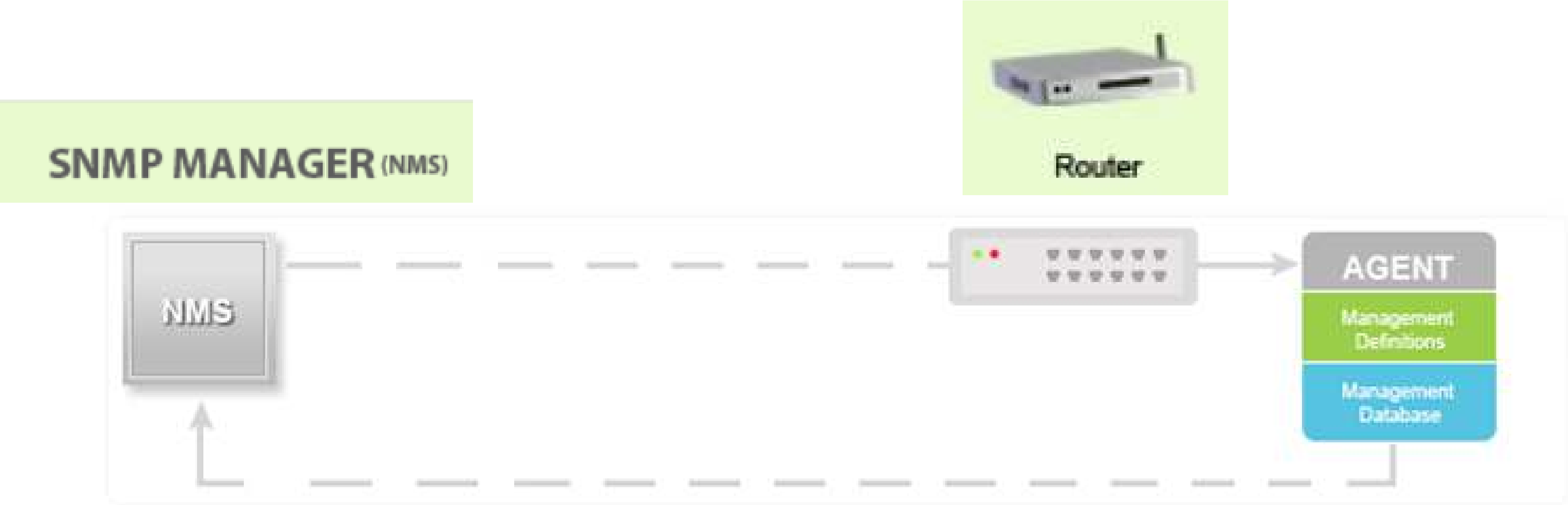

Application Layer (SNMP)

Transport Layer (UDP)

Internet Layer (IP)

Physical Layer (10 Base T)

For Example: PC running NMS to configure Router



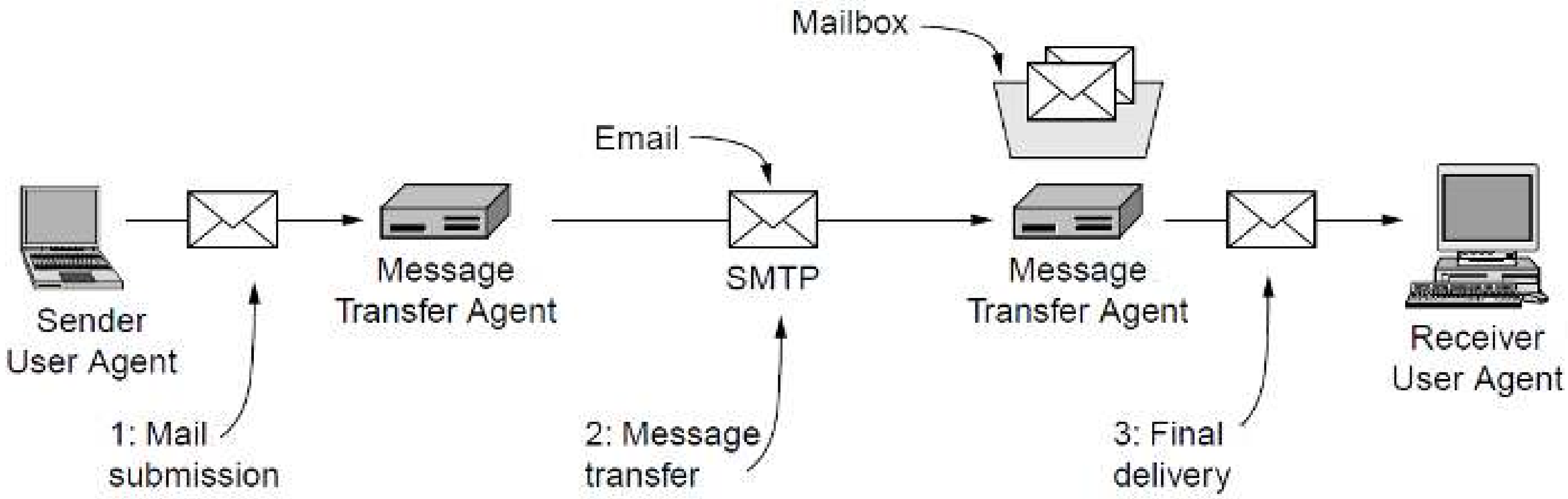
SNMP versions

Version No. - Feature
SNMP v1- implements Community–based security
SNMP v2 - implements Party–based security SNMP v2c - implements Community–based security SNMP v2u - implements User–based security
SNMP v3 - implements User–based security

Electronic mail: Architecture and Services

- Email systems consist of two subsystems: the user agents, which allow people to read and send e-mail, and the message transfer agents, which move the messages from the source to the destination.
- The user agents are local programs that provide a command based, menu-based, or graphical method for interacting with the e-mail system.
- The message transfer agents are typically system daemons, that is, processes that run in the background.
  - Their job is to move e-mail through the system.

Architecture of the Email System



Basic Functions of Email System

- Typically, e-mail systems support five basic functions:
  1. **Composition** refers to the process of creating messages and answers.
  2. **Transfer** refers to moving messages from the originator to the recipient.
  3. **Reporting** has to do with telling the originator what happened to the message.
  4. **Displaying** incoming messages is needed so people can read their e-mail.
  5. **Disposition** is the final step and concerns what the recipient does with the message after receiving it.

Additional facilities

- In addition to these basic services, some e-mail systems, especially internal corporate ones, provide a variety of advanced features like
  - mailboxes,
  - mailing lists,
  - carbon copies,
  - blind carbon copies,
  - high- priority e-mail,
  - secret (i.e., encrypted) e-mail,
  - alternative recipients if the primary one is not currently available,
  - And the ability for secretaries to read and answer their bosses' e-mail.

Message Formats

- **RFC 822**
  - Messages consist of a primitive envelope, some number of header fields, a blank line, and then the message body.
  - Each header field consists of a single line of ASCII text containing the field name, a colon, and, for most fields, a value.
- **MIME—The Multipurpose Internet Mail Extensions**
  - The basic idea of MIME is to continue to use the RFC 822 format, but to add structure to the message body and define encoding rules for non-ASCII messages.
  - By not deviating from RFC 822, MIME messages can be sent using the existing mail programs and protocols.
  - All that has to be changed are the sending and receiving programs, which users can do for themselves.
- MIME defines five new message headers.

Message Transfer Protocols

- **SMTP—The Simple Mail Transfer Protocol**
  - SMTP is an application layer protocol.
  - The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection.
  - The SMTP server is always on listening mode.
  - As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25).
  - After successfully establishing the TCP connection the client process sends the mail instantly.

- The SMTP model is of two type:
  - End-to- end method
  - Store-and- forward method

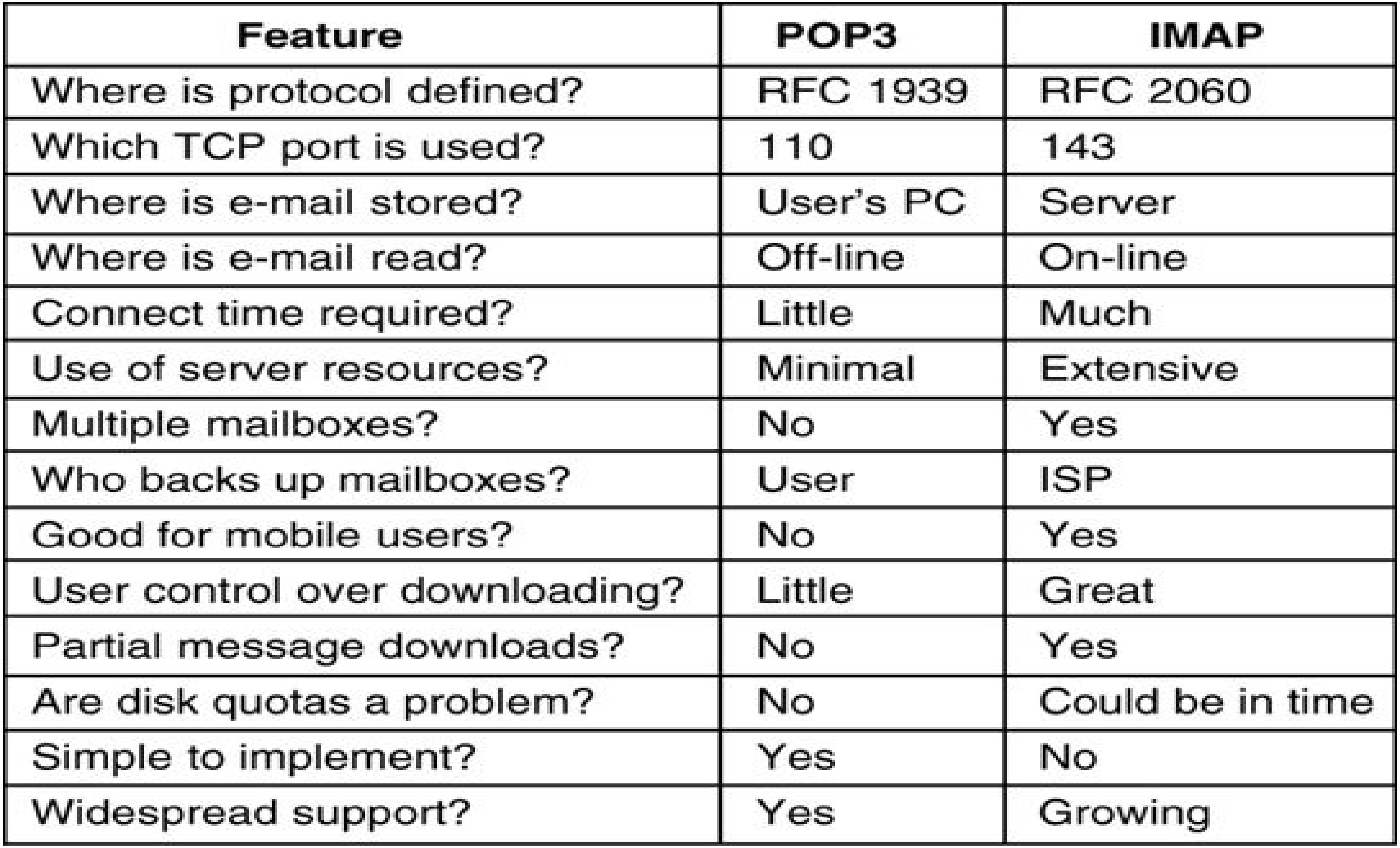
- The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization.
- A SMTP client who wants to send the mail will contact the destination’s host SMTP directly in order to send the mail to the destination.
- The SMTP server will keep the mail to itself until it is successfully copied to the receiver’s SMTP.
- The client SMTP is the one which initiates the session and the server SMTP is the one which responds to the session request.

Final Delivery

- **POP3**
  - Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client.
  - POP3 allows you to download email messages on your local computer and read them even when you are offline.
  - Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server.
  - This means that if you access your account from multiple locations, that may not be the best option for you.
  - On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

- **IMAP**
  - The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client.
  - IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails.
  - Both protocols are supported by all modern email clients and web servers.
  - While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients.
  - This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

POP3 vs. IMAP

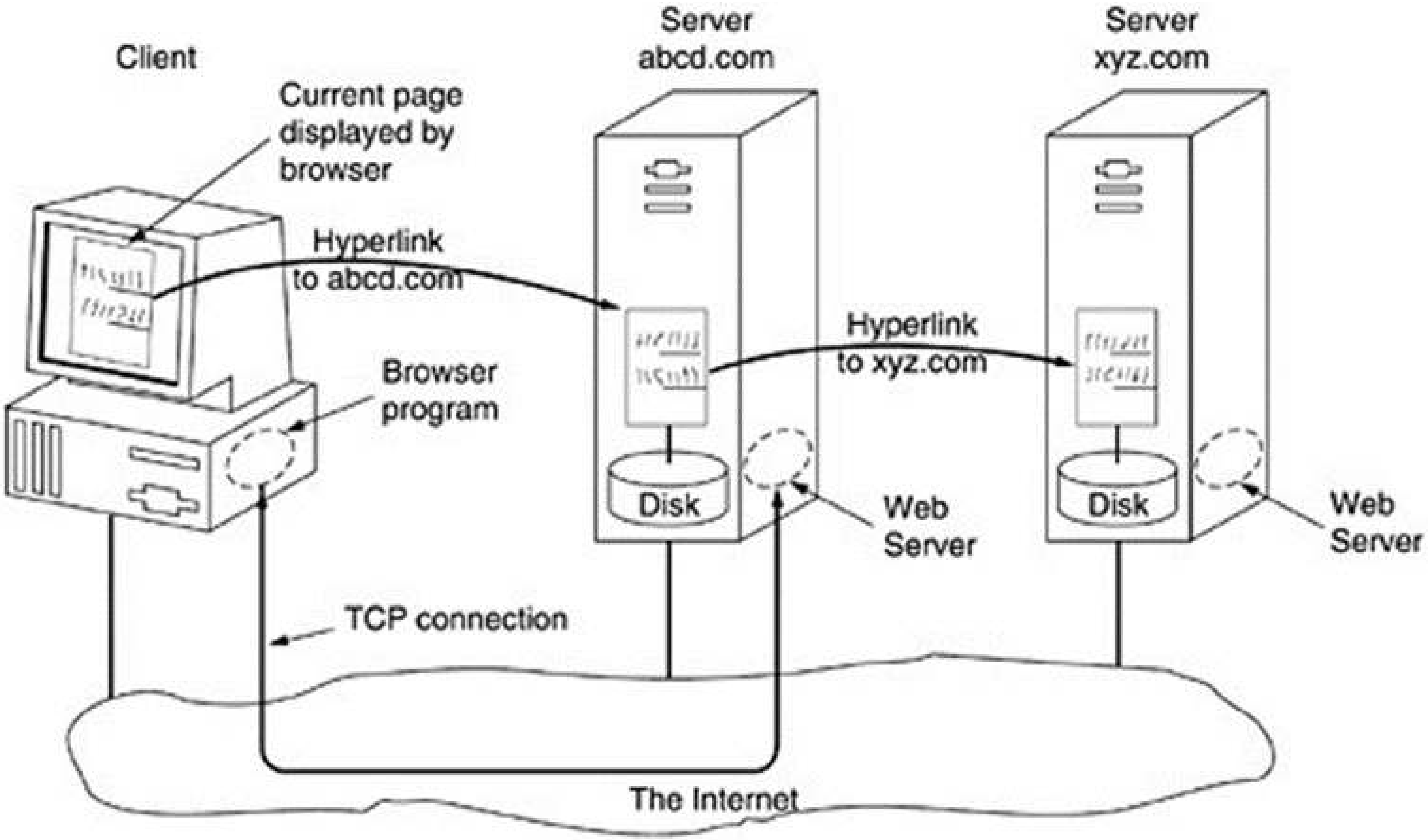


Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

World Wide Web

- The Web, or World Wide Web (W3), is basically a system of Internet servers that support specially formatted documents.
- The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files.
- This means you can jump from one document to another simply by clicking on hot spots.
- Not all Internet servers are part of the World Wide Web.

Architectural Overview



The Client Side

- A browser is a program that can display a Web page and catch mouse clicks to items on the displayed page.
- When an item is selected, the browser follows the hyperlink and fetches the page selected.
- Therefore, the embedded hyperlink needs a way to name any other page on the Web.
- Pages are named using URLs (Uniform Resource Locators).

The Server Side

- The steps that the server performs are:
  - Accept a TCP connection from a client (a browser).
  - Get the name of the file requested.
  - Get the file (from disk).
  - Return the file to the client.
  - Release the TCP connection.

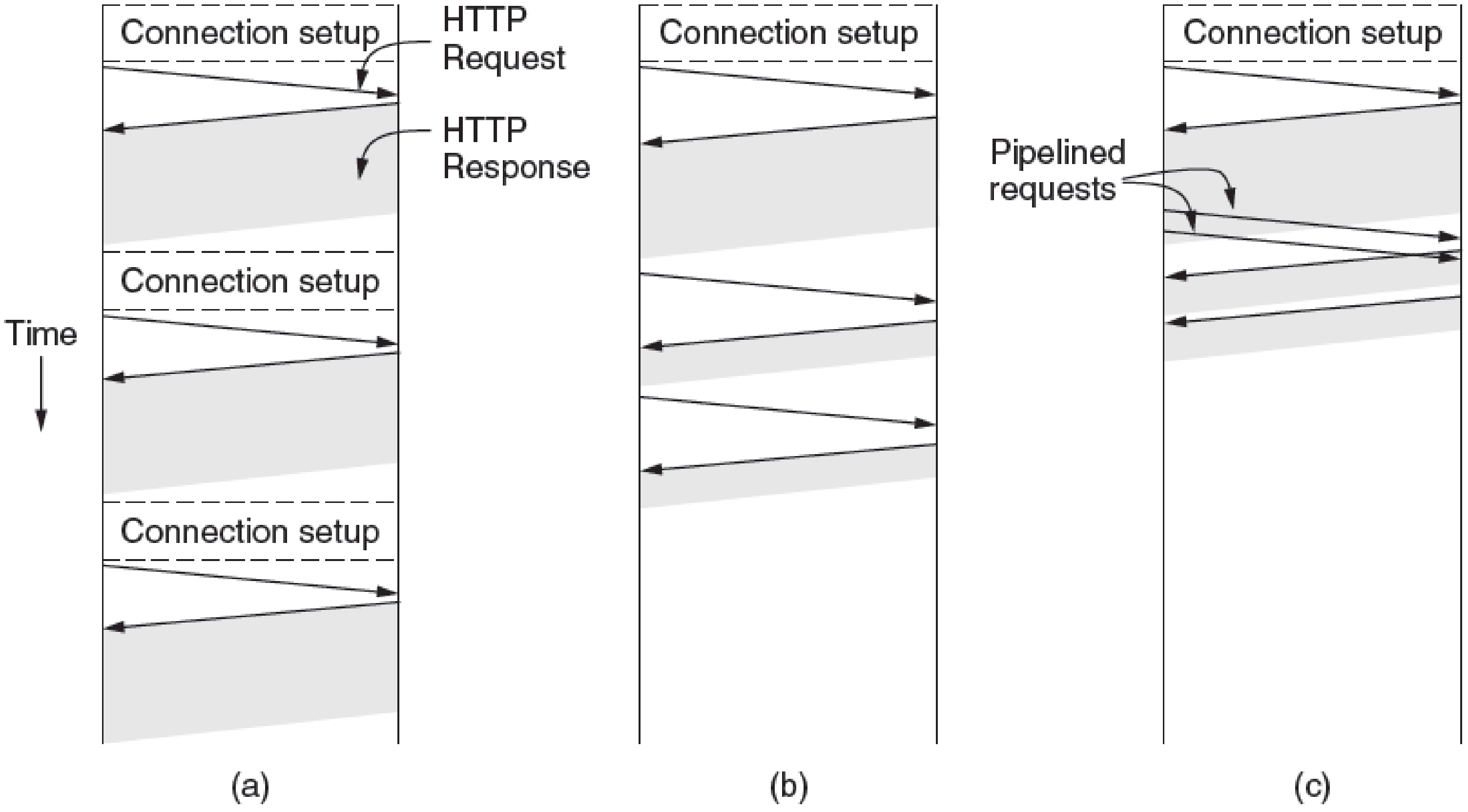
Web Page Types

- **Static Web Documents**
  - HTML
  - Forms
  - XML and XSL
- **Dynamic Web Documents**
  - Web pages often created with the help of server-side languages such as ASP, ColdFusion, Go, JavaScript, Perl, PHP, Ruby, Python, WebDNA and other languages.
- **Client-Side Dynamic Web Page Generation**
  - Client-side scripting languages like JavaScript.

HTTP: Basic Features

- **HTTP is connectionless:**
  - The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response.
  - The server processes the request and re-establishes the connection with the client to send a response back.
- **HTTP is media independent:**
  - It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content.
  - It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:**
  - HTTP is connectionless and it is a direct result of HTTP being a stateless protocol.
  - The server and client are aware of each other only during a current request.
  - Afterwards, both of them forget about each other.
  - Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

The Hypertext Transfer Protocol



(a) multiple connections and sequential requests.

(b) A persistent connection and sequential requests.

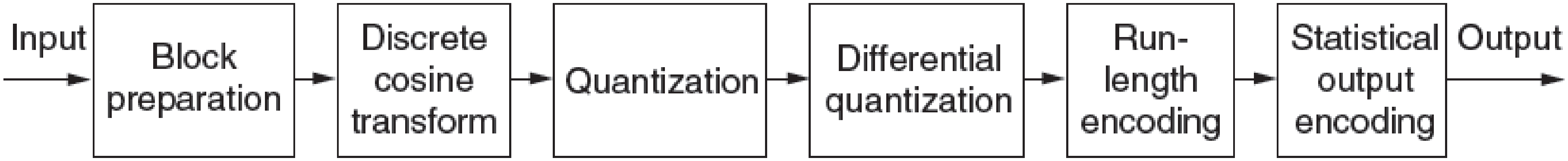
(c) A persistent connection and pipelined requests.

Digital Streaming Media

- Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a provider.
- Streaming refers to the delivery method of the medium, rather than the medium itself.
- Distinguishing delivery method from the media distributed applies specifically to telecommunications networks, as most of the delivery systems are either inherently streaming (e.g. radio, television, streaming apps) or inherently non-streaming (e.g. books, video cassettes, audio CDs).

- There are challenges with streaming content on the Internet.
- For example, users whose Internet connection lacks sufficient bandwidth may experience stops, lags, or slow buffering of the content.
- And users lacking compatible hardware or software systems may be unable to stream certain content.

Digital Video


Input
Block preparation
Discrete cosine transform
Quantization
Differential quantization
Run-length encoding
Statistical output encoding
Output

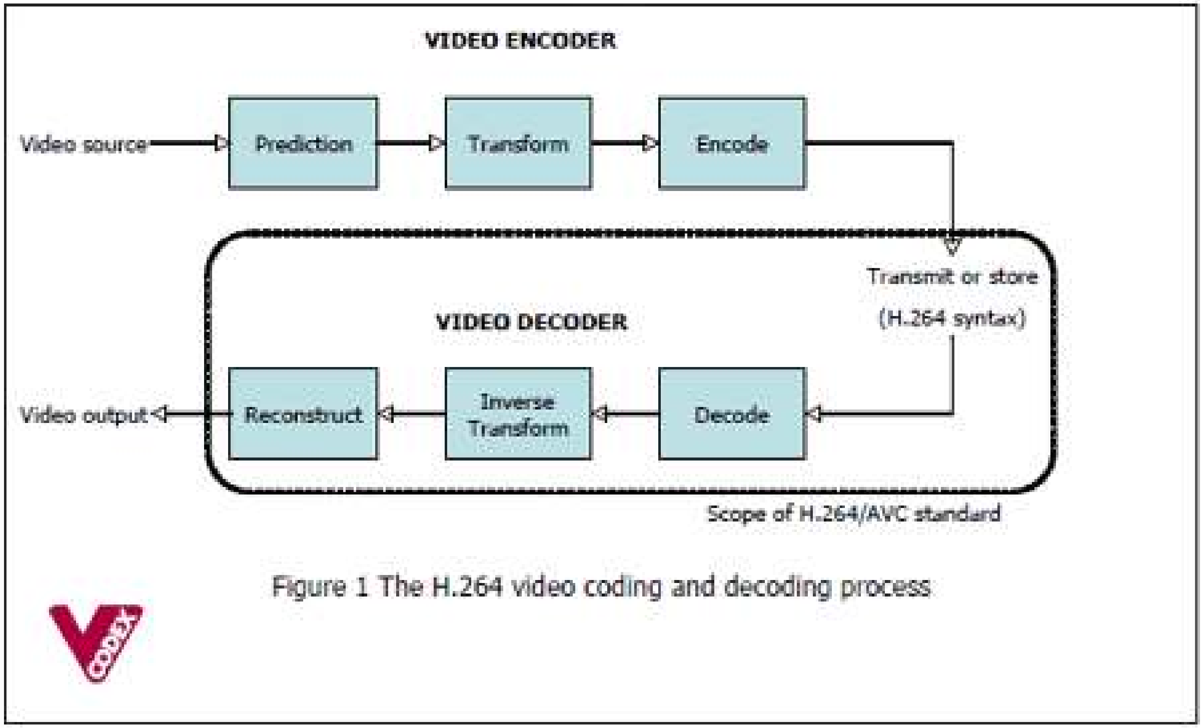
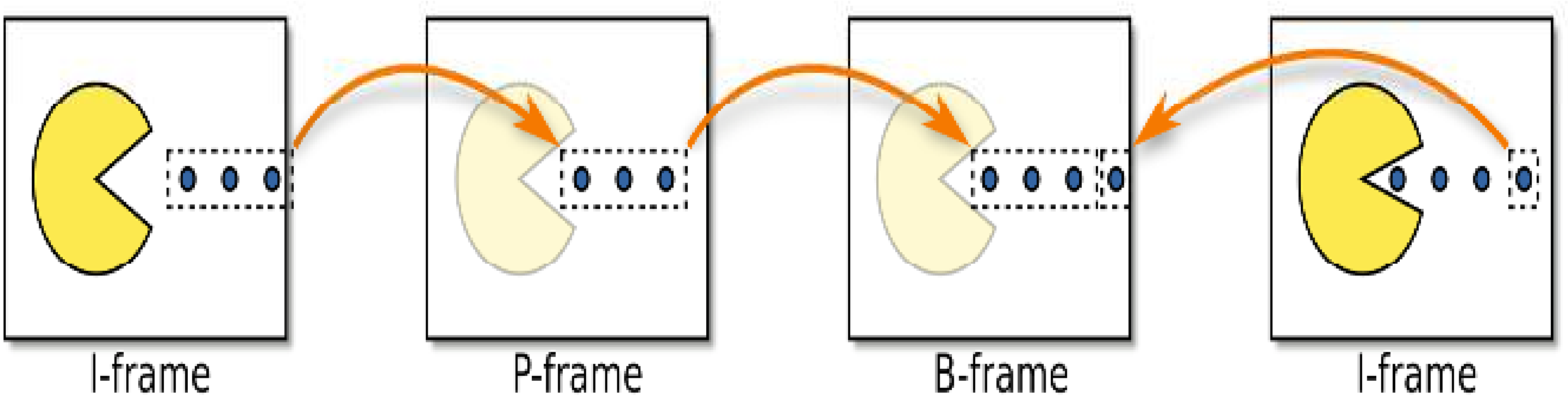


Figure 1 The H.264 video coding and decoding process

Video Compression

- Three types of pictures (or frames) are used in video compression:
  - I, P, and B frames.



Working of MPEG

- An I-frame (Intra-coded picture) is
  - a complete image, like a JPG or BMP image file.
- A P-frame (Predicted picture) holds only the changes in the image from the previous frame.
  - For example, in a scene where a car moves across a stationary background, only the car's movements need to be encoded.
  - The encoder does not need to store the unchanging background pixels in the P-frame, thus saving space.
  - P-frames are also known as delta-frames.
- A B-frame (Bidirectional predicted picture)
  - saves even more space by using differences between the current frame and both the preceding and following frames to specify its content.

Glossary of Digital audio and video

- Compression / Encoding:
  - Video information is encoded in order to transport it over the Internet and to deliver it to various kinds of video players. Compression is always a compromise between quality and file size.
- Codec:
  - The word “codec” stands for compression-decompression. A codec is a compression algorithm that is used to compress the video information at one end using an encoding program, and decompress it at the other end for playback, such as in a video player like VLC
- Format:
  - A format or “container format,” is used to bind together video and audio information, along with other information, such as metadata or even subtitles. You’ve probably heard of things like .mp4, .mov, .wmv, etc.
  - These are all container formats that put the audio and the video together.
  - For example, a .mp4 file might use the mp3 audio codec together with the H.264 video codec, or a .avi container might use AAC audio with an Xvid video codec.

- **Standard**
  - A standard, such as the MPEG standards set by the Motion Picture Experts Group, is a set of rules that video codecs and formats are designed to adhere to.
  - This standardization allows manufacturers and software designers to anticipate the kind of video, audio, and other information that their software or microchips will have to deal with.
  - For example, MPEG-1 is used in VCDs, while MPEG-2 is used in DVDs. The MPEG-4 codec, known as H.264, is the current standard used by most online video platforms.

- Bitrate
- Frame Rate
- Deinterlacing/ Decombing
- Audio Sampling Rate
- H.264
- H.265