CS8591-Computer Networks

(REGULATION 2017)

UNIT I INTRODUCTION AND PHYSICAL LAYER 9

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching.

1.1 DATA COMMUNICATIONS

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term ***telecommunication,*** which includes telephony, telegraphy, and television, means communication at a distance (*tele* is Greek for "far"). The word ***data*** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

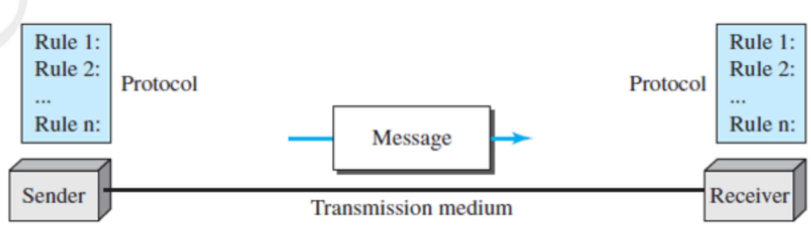
3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

1.1.1 Components

A data communications system has five components.

Figure 1.1 *Five components of data communication*



1. Message. The **message** is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The **receiver** is the device that receives the message. It can be a computer,workstation, telephone handset, television, and so on.
4. Transmission medium. The **transmission medium** is the physical path by whicha message travels from sender to receiver. Some examples of transmission mediainclude twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It representsan agreement between the communicating devices. Without a protocol, twodevices may be connected but not communicating, just as a person speaking Frenchcannot be understood by a person who speaks only Japanese.

1.2 NETWORKS

A **network** is the interconnection of a set of devices capable of communication. In thisdefinition, a device can be a **host** (or an *end system* as it is sometimes called) such as alarge computer, desktop, laptop, workstation, cellular phone, or security system. Adevice in this definition can also be a **connecting device** such as a router, which connectsthe network to other networks, a switch, which connects devices together, amodem (modulator-demodulator), which changes the form of data, and so on. Thesedevices in a network are connected using wired or wireless transmission media such ascable or air. When we connect two computers at home using a plug-and-play router, wehave created a network, although very small.

1.2.1 Network Criteria

A network must be able to meet a certain number of criteria. The most important ofthese are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time.Transit time is the amount of time required for a message to travel from one device toanother. Response time is the elapsed time between an inquiry and a response. The performanceof a network depends on a number of factors, including the number of users,the type of transmission medium, the capabilities of the connected hardware, and theefficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay.**We often need more throughput and less delay. However, these two criteria are oftencontradictory. If we try to send more data to the network, we may increase throughputbut we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network **reliability** is measured by the frequency offailure, the time it takes a link to recover from a failure, and the network's robustness ina catastrophe.

Security

Network **security** issues include protecting data from unauthorized access, protectingdata from damage and development, and implementing policies and procedures forrecovery from breaches and data losses.

1.2.2 Physical Structures

Before discussing networks, we need to define some network attributes.

Type of Connection

A network is two or more devices connected through links. A link is a communicationspathway that transfers data from one device to another. For visualization purposes, it issimplest to imagine any link as a line drawn between two points. For communication tooccur, two devices must be connected in some way to the same link at the same time.

There are two possible types of connections: point-to-point and multipoint.

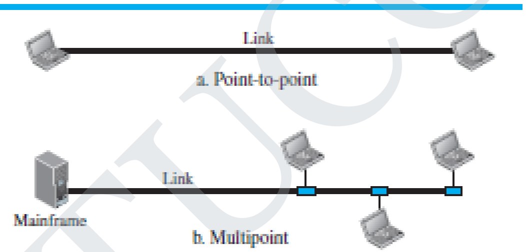
Point-to-Point

A **point-to-point connection** provides a dedicated link between two devices. Theentire capacity of the link is reserved for transmission between those two devices. Mostpoint-to-point connections use an actual length of wire or cable to connect the twoends, but other options, such as microwave or satellite links, are also possible. When we change television channels by infrared remote control, we areestablishing a point-to-point connection between the remote control and the television'scontrol system.

Multipoint

A **multipoint** (also called **multidrop**) **connection** is one in which more than two specificdevices share a single link. The capacity of the channel is shared spatially or temporally.

Types of connections: point-to-point and multipoint



Physical Topology

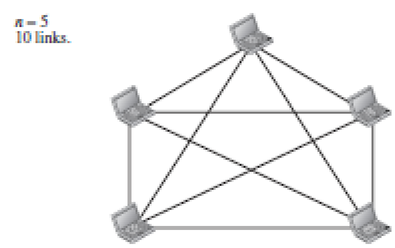
The term ***physical topology*** refers to the way in which a network is laid out physically.Two or more devices connect to a link; two or more links form a topology. The topologyof a network is the geometric representation of the relationship of all the links andlinking devices (usually called ***nodes***) to one another. There are four basic topologiespossible: mesh, star, bus, and ring.

Mesh Topology

In a **mesh topology,** every device has a dedicated point-to-point link to every otherdevice. The term *dedicated* means that the link carries traffic only between the twodevices it connects. To find the number of physical links in a fully connected mesh networkwith *n* nodes, we first consider that each node must be connected to every othernode. Node 1 must be connected to *n* –

1 nodes, node 2 must be connected to *n* – 1nodes, and finally node *n* must be connected to *n* – 1 nodes. We need *n* (*n* – 1) physicallinks.

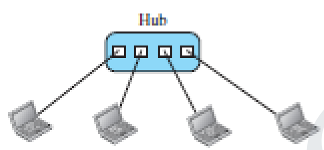
A fully connected mesh topology (five devices)



Star Topology

In a **star topology**, each device has a dedicated point-to-point link only to a central controller,usually called a hub. The devices are not directly linked to one another. Unlike amesh topology, a star topology does not allow direct traffic between devices. The controlleracts as an exchange: If one device wants to send data to another, it sends thedata to the controller, which then relays the data to the other connected device.

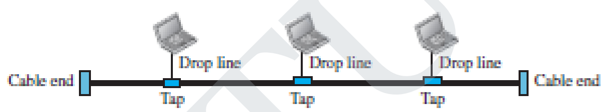
A star topology connecting four stations



Bus Topology

The preceding examples all describe point-to-point connections. A **bus topology,** on theother hand, is multipoint. One long cable acts as a **backbone** to link all the devices in anetwork .

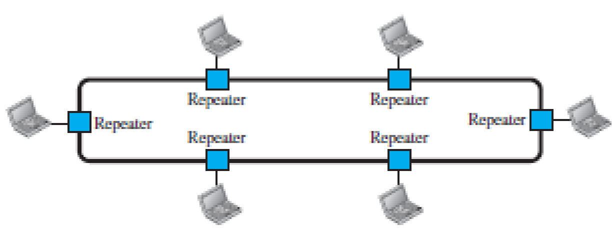
A bus topology connecting three stations



Ring Topology

In a **ring topology,** each device has a dedicated point-to-point connection with only thetwo devices on either side of it. A signal is passed along the ring in one direction, fromdevice to device, until it reaches its destination. Each device in the ring incorporates arepeater. When a device receives a signal intended for another device, its repeaterregenerates the bits and passes them along.

A ring topology connecting six stations

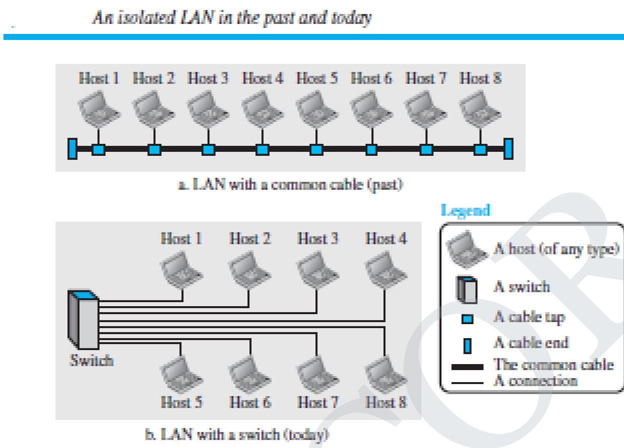


1.3 NETWORK TYPES

The criterion of distinguishing one type of network from another is difficult and sometimes confusing.We use a few criteria such as size, geographical coverage, and ownership to make thisdistinction. After discussing two types of networks, LANs and WANs, we define switching,which is used to connect networks to form an internetwork (a network of networks).

1.3.1 Local Area Network

A **local area network** (**LAN**) is usually privately owned and connects some hosts in asingle office, building, or campus. Depending on the needs of an organization, a LANcan be as simple as two PCs and a printer in someone's home office, or it can extendthroughout a company and include audio and video devices. Each host in a LAN has anidentifier, an address, that uniquely defines the host in the LAN. A packet sent by a hostto another host carries both the source host's and the destination host's addresses.



1.3.2 Wide Area Network

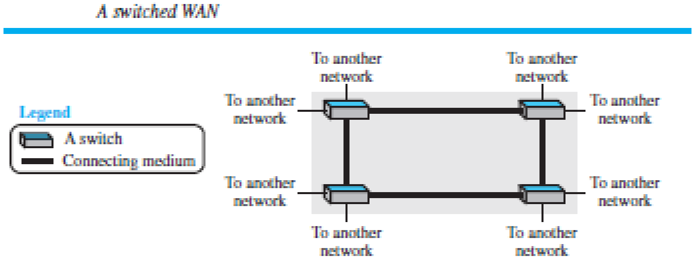
A **wide area network (WAN)** is also an interconnection of devices capable of communication.However, there are some differences between a LAN and a WAN. A LAN is normallylimited in size, spanning an office, a building, or a campus; a WAN has a wider geographicalspan, spanning a town, a state, a country, or even the world. A LAN interconnects hosts;a WAN interconnects connecting devices such as switches, routers, or modems. A LAN isnormally privately owned by the organization that uses it; a WAN is normally created andrun by communication companies and leased by an organization that uses it. Two distinct examples of WANs today: point-to-point WANs and switched WANs.

Point-to-Point WAN

A point-to-point WAN is a network that connects two communicating devices through a transmissionmedia (cable or air).

Switched WAN

A switched WAN is a network with more than two ends. A switched WAN, is used in the backbone of global communication today. Switched WAN is a combination of several point-to-point WANs that are connected by switches.



Internetwork

Today, it is very rare to see a LAN or a WAN in isolation; they are connected to oneanother. When two or more networks are connected, they make an **internetwork,** or**internet.**

1.3.3 Switching

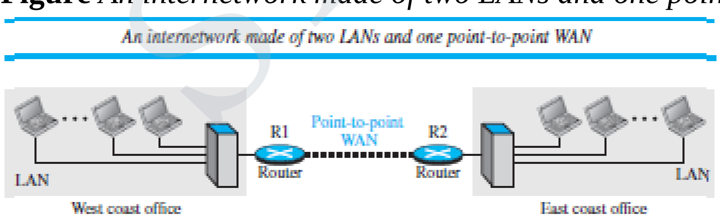
An internet is a **switched network** in which a switch connects at least two linkstogether. A switch needs to forward data from a network to another network whenrequired. The two most common types of switched networks are circuit-switched andpacket-switched networks. We discuss both next.

Circuit-Switched Network

In a **circuit-switched network,** a dedicated connection, called a circuit, is alwaysavailable between the two end systems; the switch can only make it active or inactive.Figure, shows a very simple switched network that connects four telephones toeach end. We have used telephone sets instead of computers as an end system becausecircuit switching was very common in telephone networks in the past, although part ofthe telephone network today is a packet-switched network.

In Figure the four telephones at each side are connected to a switch. Theswitch connects a telephone set at one side to a telephone set at the other side. The thickline connecting two switches is a high-capacity communication line that can handlefour voice communications at the same time; the capacity can be shared between allpairs of telephone sets. The switches used in this example have forwarding tasks but nostoring capability.

Figure *An internetwork made of two LANs and one point-to-point WAN*



Let us look at two cases. In the first case, all telephone sets are busy; four people atone site are talking with four people at the other site; the capacity of the thick line isfully used. In the second case, only one telephone set at one side is connected to a telephoneset at the other side; only one-fourth of the capacity of the thick line is used. Thismeans that a circuit-switched network is efficient only when it is working at its fullcapacity; most of the time, it is inefficient because it is working at partial capacity. Thereason that we need to make the capacity of the thick line four times the capacity ofeach voice line is that we do not want communication to fail when all telephone sets atone side want to be connected with all telephone sets at the other side.

Figure *A heterogeneous network made of four WANs and three LANs*

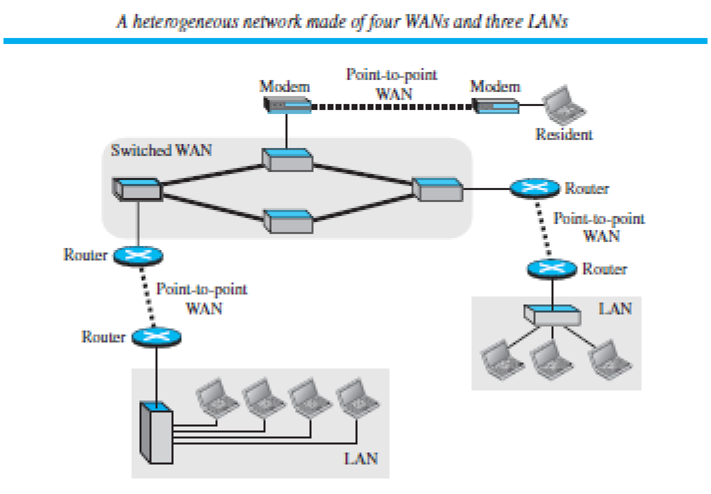
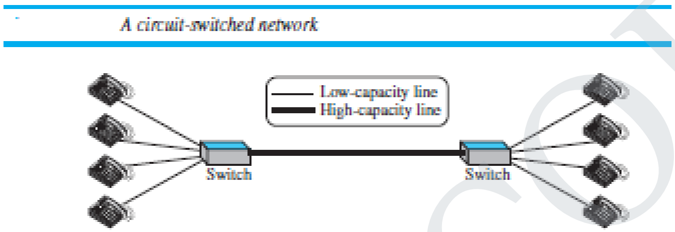


Figure *A circuit-switched network*



Packet-Switched Network

In a computer network, the communication between the two ends is done in blocks ofdata called **packets.** In other words, instead of the continuous communication we seebetween two telephone sets when they are being used, we see the exchange of individualdata packets between the two computers. This allows us to make the switches functionfor both storing and forwarding because a packet is an independent entity that canbe stored and sent later.

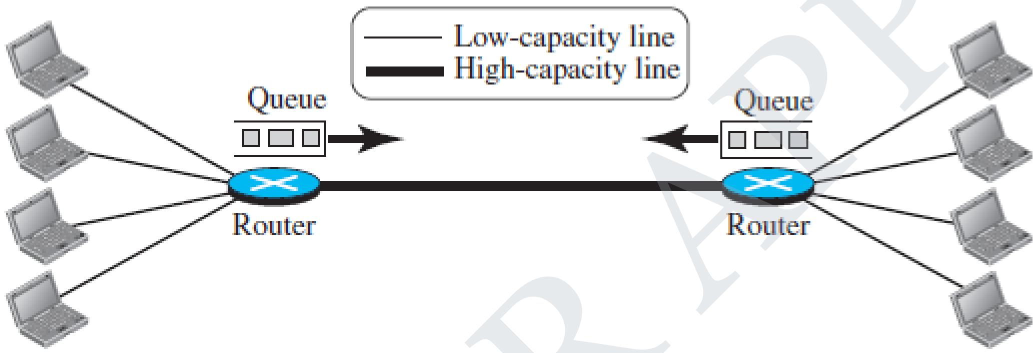
A router in a packet-switched network has a queue that can store and forward thepacket. Now assume that the capacity of the thick line is only twice the capacity of thedata line connecting the computers to the routers. If only two computers (one at eachsite) need to communicate with each other, there is no waiting for the packets.

However, if packets arrive at one router when the thick line is already working at its fullcapacity, the packets should be stored and forwarded in the order they arrived. The twosimple examples show that a packet-switched network is more efficient than a circuitswitchednetwork, but the packets may encounter some delays.

1.3.4 The Internet

An internet (note the lowercase *i*) is two or more networks thatcan communicate with each other. The most notable internet is called the **Internet**(uppercase *I*), and is composed of thousands of interconnected networks. The figure shows the Internet as several backbones, provider networks, and customernetworks. At the top level, the *backbones* are large networks owned by somecommunication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbonenetworks are connected through some complex switching systems, called *peeringpoints*. At the second level, there are smaller networks, called *provider networks*, thatuse the services of the backbones for a fee. The provider networks are connected tobackbones and sometimes to other provider networks. The *customer networks* are

A packet-switched network



networks at the edge of the Internet that actually use the services provided by the Internet.They pay fees to provider networks for receiving services.Backbones and provider networks are also called **Internet Service Providers(ISPs).** The backbones are often referred to as *international ISPs;* the provider networksare often referred to as *national* or *regional ISPs*.

1.3.5 Accessing the Internet

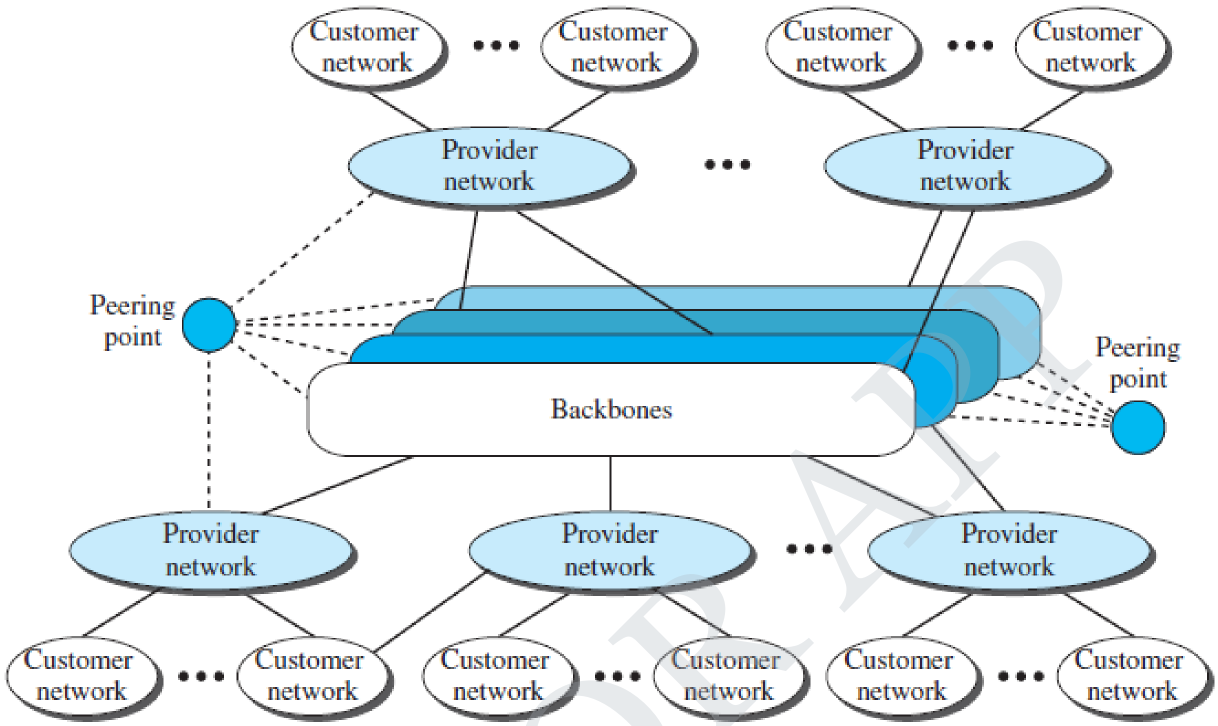
The Internet today is an internetwork that allows any user to become part of it. Theuser, however, needs to be physically connected to an ISP. The physical connection isnormally done through a point-to-point WAN.

Using Telephone Networks

Today most residences and small businesses have telephone service, which meansthey are connected to a telephone network. Since most telephone networks havealready connected themselves to the Internet, one option for residences and smallbusinesses to connect to the Internet is to change the voice line between the residenceor business and the telephone center to a point-to-point WAN. This can be done intwo ways.

❑ ***Dial-up service.***The first solution is to add to the telephone line a modem thatconverts data to voice. The software installed on the computer dials the ISP andimitates making a telephone connection. Unfortunately, the dial-up service isvery slow, and when the line is used for Internet connection, it cannot be used fortelephone (voice) connection. It is only useful for small residences.

The Internet today



❑***DSL Service.***Since the advent of the Internet, some telephone companies haveupgraded their telephone lines to provide higher speed Internet services to residencesor small businesses. The DSL service also allows the line to be used simultaneouslyfor voice and data communication.

Using Cable Networks

More and more residents over the last two decades have begun using cable TV servicesinstead of antennas to receive TV broadcasting. The cable companies have beenupgrading their cable networks and connecting to the Internet. A residence or a smallbusiness can be connected to the Internet by using this service. It provides a higherspeed connection, but the speed varies depending on the number of neighbors that usethe same cable.

Using Wireless Networks

Wireless connectivity has recently become increasingly popular. A household or asmall business can use a combination of wireless and wired connections to access theInternet. With the growing wireless WAN access, a household or a small business canbe connected to the Internet through a wireless WAN.

Direct Connection to the Internet

A large organization or a large corporation can itself become a local ISP and be connectedto the Internet. This can be done if the organization or the corporation leases ahigh-speed WAN from a carrier provider and connects itself to a regional ISP. Forexample, a large university with several campuses can create an internetwork and thenconnect the internetwork to the Internet.

1.4 PROTOCOL LAYERING

In data communication and networking, aprotocol defines the rules that both the sender and receiver and all intermediate devicesneed to follow to be able to communicate effectively. When communication is simple,we may need only one simple protocol; when the communication is complex, we mayneed to divide the task between different layers, in which case we need a protocol ateach layer, or **protocol layering.**

1.4.1 Scenarios

Let us develop two simple scenarios to better understand the need for protocol layering.

First Scenario

In the first scenario, communication is so simple that it can occur in only one layer.Assume Maria and Ann are neighbors with a lot of common ideas. Communicationbetween Maria and Ann takes place in one layer, face to face, in the same language, asshown in Figure.

Even in this simple scenario, we can see that a set of rules needs to be followed.First, Maria and Ann know that they should greet each other when they meet. Second,they know that they should confine their vocabulary to the level of their friendship.Third, each party knows that she should refrain from speaking when the other partyis speaking. Fourth, each party knows that the conversation should be a dialog, not amonolog: both should have the opportunity to talk about the issue. Fifth, they shouldexchange some nice words when they leave.

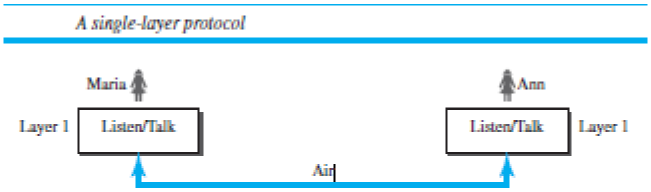
We can see that the protocol used by Maria and Ann is different from the communicationbetween a professor and the students in a lecture hall. The communication inthe second case is mostly monolog; the professor talks most of the time unless a studenthas a question, a situation in which the protocol dictates that she should raise her handand wait for permission to speak. In this case, the communication is normally very formaland limited to the subject being taught.

Second Scenario

In the second scenario, we assume that Ann is offered a higher-level position in hercompany, but needs to move to another branch located in a city very far from Maria.The two friends still want to continue their communication and exchange ideas becausethey have come up with an innovative project to start a new business when they bothretire. They decide to continue their conversation using regular mail through the postoffice. However, they do not want their ideas to be revealed by other people if the lettersare intercepted. They agree on an encryption/decryption technique. The sender ofthe letter encrypts it to make it unreadable by an intruder; the receiver of the letterdecrypts it to get the original letter.

Now wecan say that the communication between Maria and Ann takes place in three layers, asshown in Figure 2.2. We assume that Ann and Maria each have three machines (orrobots) that can perform the task at each layer.

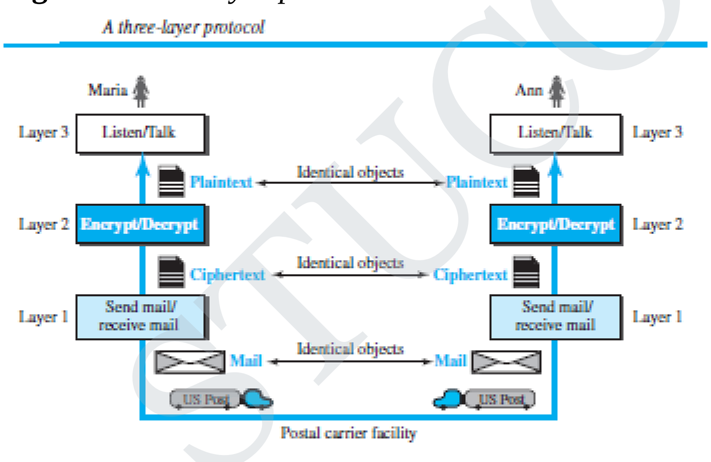
Figure *A single-layer protocol*



Let us assume that Maria sends the first letter to Ann. Maria talks to the machine atthe third layer as though the machine is Ann and is listening to her. The third layermachine listens to what Maria says and creates the plaintext (a letter in English), whichis passed to the second layer machine. The second layer machine takes the plaintext,encrypts it, and creates the ciphertext, which is passed to the first layer machine. Thefirst layer machine, presumably a robot, takes the ciphertext, puts it in an envelope,adds the sender and receiver addresses, and mails it.

At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizingthe letter from Maria by the sender address. The machine takes out the ciphertextfrom the envelope and delivers it to the second layer machine. The second layermachine decrypts the message, creates the plaintext, and passes the plaintext to thethird-layer machine. The third layer machine takes the plaintext and reads it as thoughMaria is speaking.

Figure *A three-layer protocol*



Protocol layering enables us to divide a complex task into several smaller and simplertasks. For example, in Figure 2.2, we could have used only one machine to do thejob of all three machines. However, if Maria and Ann decide that the encryption/decryption done by the machine is not enough to protect their secrecy, they would haveto change the whole machine. In the present situation, they need to change only the secondlayer machine; the other two can remain the same. This is referred to as *modularity*.Modularity in this case means independent layers. A layer (module) can be defined as ablack box with inputs and outputs, without concern about how inputs are changed tooutputs. If two machines provide the same outputs when given the same inputs, theycan replace each other. For example, Ann and Maria can buy the second layer machinefrom two different manufacturers. As long as the two machines create the same ciphertextfrom the same plaintext and vice versa, they do the job.

Advantages of protocol layering:

It allows us to separate theservices from the implementation.

A layer needs to be able to receive a set of servicesfrom the lower layer and to give the services to the upper layer;

Communicationdoes not always use only two end systems; there are intermediate systems thatneed only some layers, but not all layers. If we did not use protocol layering, we wouldhave to make each intermediate system as complex as the end systems, which makesthe whole system more expensive.

Disadvantage to protocol layering?

One can argue that having a singlelayer makes the job easier. There is no need for each layer to provide a service to theupper layer and give service to the lower layer. For example, Ann and Maria could findor build one machine that could do all three tasks. However, as mentioned above, if oneday they found that their code was broken, each would have to replace the wholemachine with a new one instead of just changing the machine in the second layer.

1.4.2 Principles of Protocol Layering

Let us discuss two principles of protocol layering.

First Principle

The first principle dictates that if we want bidirectional communication, we need tomake each layer so that it is able to perform two opposite tasks, one in each direction.For example, the third layer task is to listen (in one direction) and *talk* (in the otherdirection). The second layer needs to be able to encrypt and decrypt. The first layerneeds to send and receive mail.

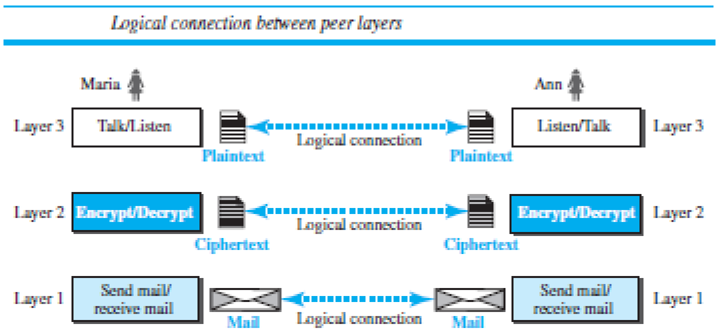
Second Principle

The second principle that we need to follow in protocol layering is that the twoobjects under each layer at both sites should be identical. For example, the objectunder layer 3 at both sites should be a plaintext letter. The object under layer 2 atboth sites should be a ciphertext letter. The object under layer 1 at both sites shouldbe a piece of mail.

1.4.3 Logical Connections

After following the above two principles, we can think about logical connectionbetween each layer as shown in Figure. This means that we have layer-to-layercommunication. Maria and Ann can think that there is a logical (imaginary) connectionat each layer through which they can send the object created from that layer.

Figure *Logical connection between peer layers*



1.5 TCP/IP PROTOCOL SUITE

Now that we know about the concept of protocol layering and the logical communicationbetween layers in our second scenario, we can introduce the TCP/IP (TransmissionControl Protocol/Internet Protocol). TCP/IP is a protocol suite (a set of protocols organizedin different layers) used in the Internet today. It is a hierarchical protocol made upof interactive modules, each of which provides a specific functionality. The term *hierarchical*means that each upper level protocol is supported by the services provided byone or more lower level protocols. The original TCP/IP protocol suite was defined asfour software layers built upon the hardware. Today, however, TCP/IP is thought of as afive-layer model.

1.5.1 Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in communicationbetween two hosts, we assume that we want to use the suite in a small internet made upof three LANs (links), each with a link-layer switch. We also assume that the links areconnected by one router.

Let us assume that computer A communicates with computer B. As the figureshows, we have five communicating devices in this communication: source host(computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2,and the destination host (computer B). Each device is involved with a set of layersdepending on the role of the device in the internet. The two hosts are involved in all fivelayers; the source host needs to create a message in the application layer and send itdown the layers so that it is physically sent to the destination host. The destination hostneeds to receive the communication at the physical layer and then deliver it through theother layers to the application layer.

Figure *Layers in the TCP/IP protocol suite*

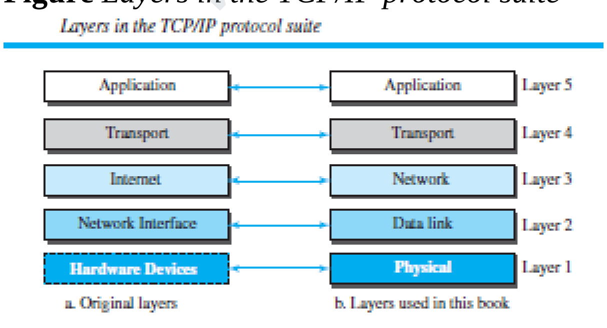
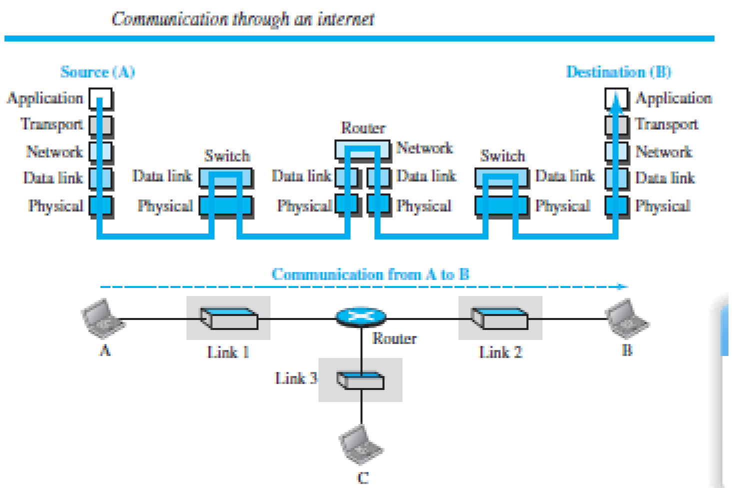


Figure *Communication through an internet*



The router is involved in only three layers; there is no transport or application layerin a router as long as the router is used only for routing. Although a router is alwaysinvolved in one network layer, it is involved in *n* combinations of link and physical layersin which *n* is the number of links the router is connected to. The reason is that eachlink may use its own data-link or physical protocol. For example, in the above figure, therouter is involved in three links, but the message sent from source A to destination B isinvolved in two links. Each link may be using different link-layer and physical-layerprotocols; the router needs to receive a packet from link 1 based on one pair of protocolsand deliver it to link 2 based on another pair of protocols.

A link-layer switch in a link, however, is involved only in two layers, data-link andphysical. Although each switch in the above figure has two different connections, theconnections are in the same link, which uses only one set of protocols. This means that,unlike a router, a link-layer switch is involved only in one data-link and one physicallayer.

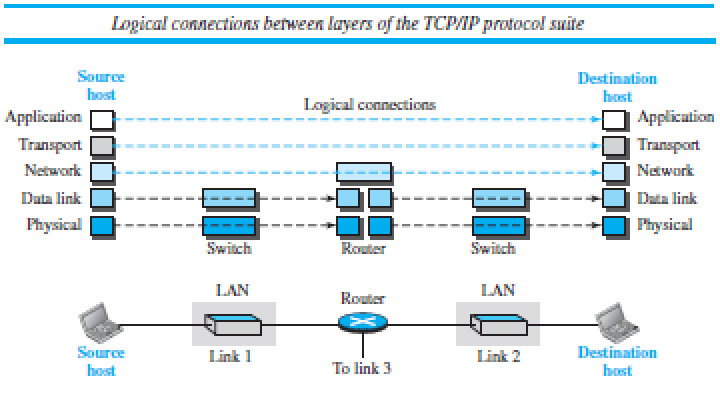
1.5.2 Layers in the TCP/IP Protocol Suite

After the above introduction, we briefly discuss the functions and duties of layers inthe TCP/IP protocol suite. Each layer is discussed in detail in the next five parts ofthe book. To better understand the duties of each layer, we need to think about thelogical connections between layers.

Using logical connections makes it easier for us to think about the duty of eachlayer. As the figure shows, the duty of the application, transport, and network layers isend-to-end. However, the duty of the data-link and physical layers is hop-to-hop, inwhich a hop is a host or router. In other words, the domain of duty of the top threelayers is the internet, and the domain of duty of the two lower layers is the link.

Another way of thinking of the logical connections is to think about the data unitcreated from each layer. In the top three layers, the data unit (packets) should not bechanged by any router or link-layer switch. In the bottom two layers, the packet createdby the host is changed only by the routers, not by the link-layer switches.

Figure *Logical connections between layers of the TCP/IP protocol suite*

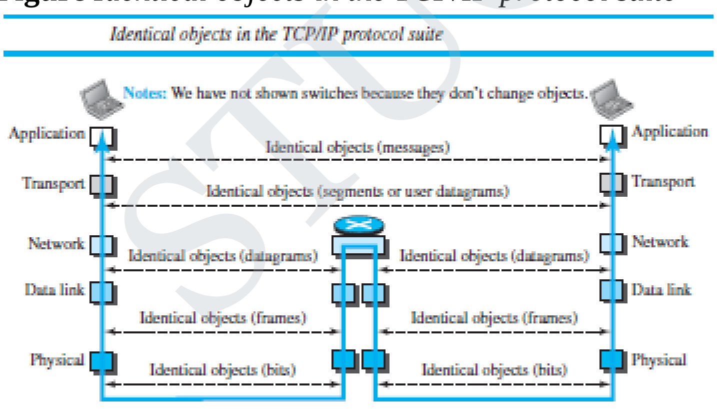


1.5.3 Description of Each Layer

Physical Layer

We can say that the physical layer is responsible for carrying individual bits in a frameacross the link. Although the physical layer is the lowest level in the TCP/IP protocolsuite, the communication between two devices at the physical layer is still a logicalcommunication because there is another, hidden layer, the transmission media, underthe physical layer. Two devices are connected by a transmission medium (cable or air).We need to know that the transmission medium does not carry bits; it carries electricalor optical signals. So the bits received in a frame from the data-link layer are transformedand sent through the transmission media, but we can think that the logical unitbetween two physical layers in two devices is a *bit*. There are several protocols thattransform a bit to a signal. We discuss them in Part II when we discuss the physicallayer and the transmission media.

Figure *Identical objects in the TCP/IP protocol suite*



Data-link Layer

We have seen that an internet is made up of several links (LANs and WANs) connectedby routers. There may be several overlapping sets of links that a datagram can travelfrom the host to the destination. The routers are responsible for choosing the *best* links.However, when the next link to travel is determined by the router, the data-link layer isresponsible for taking the datagram and moving it across the link. The link can be awired LAN with a link-layer switch, a wireless

LAN, a wired WAN, or a wirelessWAN. We can also have different protocol used with any link type. In each case, thedata-link layer is responsible for moving the packet through the link.TCP/IP does not define any specific protocol for the data-link layer. It supports allthe standard and proprietary protocols. Any protocol that can take the datagram andcarry it through the link suffices for the network layer. The data-link layer takes a datagramand encapsulates it in a packet called a *frame*.Each link-layer protocol may provide a different service. Some link-layer protocolsprovide complete error detection and correction, some provide only error correction.

Network Layer

The network layer is responsible for creating a connection between the source computerand the destination computer. The communication at the network layer is host-to-host.However, since there can be several routers from the source to the destination, the routersin the path are responsible for choosing the best route for each packet. We can say that thenetwork layer is responsible for host-to-host communication and routing the packetthrough possible routes. Again, we may ask ourselves why we need the network layer. Wecould have added the routing duty to the transport layer and dropped this layer. One reason,as we said before, is the separation of different tasks between different layers. The secondreason is that the routers do not need the application and transport layers. Separating thetasks allows us to use fewer protocols on the routers.

The network layer in the Internet includes the main protocol, Internet Protocol(IP), that defines the format of the packet, called a datagram at the network layer. IPalso defines the format and the structure of addresses used in this layer. IP is alsoresponsible for routing a packet from its source to its destination, which is achieved byeach router forwarding the datagram to the next router in its path.IP is a connectionless protocol that provides no flow control, no error control, andno congestion control services. This means that if any of theses services is required foran application, the application should rely only on the transport-layer protocol. The networklayer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.A routing protocol does not take part in routing (it is the responsibility of IP),but it creates forwarding tables for routers to help them in the routing process.The network layer also has some auxiliary protocols that help IP in its delivery androuting tasks. The Internet Control Message Protocol (ICMP) helps IP to report someproblems when routing a packet. The Internet Group Management Protocol (IGMP) isanother protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol(DHCP) helps IP to get the network-layer address for a host. The Address ResolutionProtocol (ARP) is a protocol that helps IP to find the link-layer address of a host ora router when its network-layer address is given.

Transport Layer

The logical connection at the transport layer is also end-to-end. The transport layer at thesource host gets the message from the application layer, encapsulates it in a transportlayerpacket (called a *segment* or a *user datagram* in different protocols) and sends it,through the logical (imaginary) connection, to the transport layer at the destination host.In other words, the transport layer is responsible for giving services to the applicationlayer: to get a message from an application program running on the source host anddeliver it to the corresponding application program on the destination host. We may askwhy we need an end-to-end transport layer when we already have an end-to-end applicationlayer. The reason is the separation of tasks and duties, which we discussed earlier.The transport layer should be independent of the application layer. In addition, we willsee that we have more than one protocol in the transport layer, which means that eachapplication program can use the protocol that best matches its requirement.

As we said, there are a few transport-layer protocols in the Internet, each designedfor some specific task. The main protocol, Transmission Control Protocol (TCP), is aconnection-oriented protocol that first establishes a logical connection between transportlayers at two hosts before transferring data. It creates a logical pipe between twoTCPs for transferring a stream of bytes. TCP provides flow control (matching the sendingdata rate of the source host with the receiving data rate of the destination host toprevent overwhelming the destination), error control (to guarantee that the segmentsarrive at the destination without error and resending the corrupted ones), and congestioncontrol to reduce the loss of segments due to congestion in the network. The othercommon protocol, User Datagram Protocol (UDP), is a connectionless protocol thattransmits user datagrams without first creating a logical connection. In UDP, each user datagram is an independent entity without being related to the previous or the next one(the meaning of the term *connectionless*). UDP is a simple protocol that does not provideflow, error, or congestion control. Its simplicity, which means small overhead, isattractive to an application program that needs to send short messages and cannotafford the retransmission of the packets involved in TCP, when a packet is corrupted orlost. A new protocol, Stream Control Transmission Protocol (SCTP) is designed torespond to new applications that are emerging in the multimedia.

Application Layer

As Figure 2.6 shows, the logical connection between the two application layers is endto-end. The two application layers exchange *messages* between each other as thoughthere were a bridge between the two layers. However, we should know that the communicationis done through all the layers.Communication at the application layer is between two *processes* (two programsrunning at this layer). To communicate, a process sends a request to the other processand receives a response. Process-to-process communication is the duty of the applicationlayer. The application layer in the Internet includes many predefined protocols, buta user can also create a pair of processes to be run at the two hosts.

The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the WorldWide Web (WWW). The Simple Mail Transfer Protocol (SMTP) is the main protocolused in electronic mail (e-mail) service. The File Transfer Protocol (FTP) is used fortransferring files from one host to another. The Terminal Network (TELNET) andSecure Shell (SSH) are used for accessing a site remotely. The Simple Network ManagementProtocol (SNMP) is used by an administrator to manage the Internet at globaland local levels. The Domain Name System (DNS) is used by other protocols to findthe network-layer address of a computer. The Internet Group Management Protocol(IGMP) is used to collect membership in a group.

1.5.4 Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/decapsulation. We have not shown the layers for the link-layer switches because no encapsulation/decapsulationoccurs in this device.

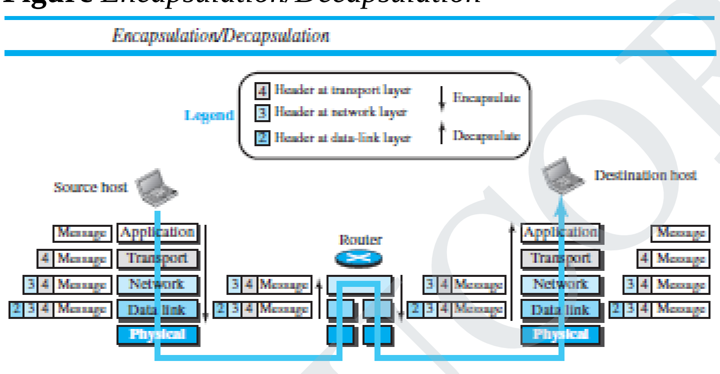
Encapsulation at the Source Host

At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a *message*. Amessage normally does not contain any header or trailer, but if it does, we refer tothe whole as the message. The message is passed to the transport layer.

2. The transport layer takes the message as the payload, the load that the transportlayer should take care of. It adds the transport layer header to the payload, whichcontains the identifiers of the source and destination application programs thatwant to communicate plus some more information that is needed for the end-toenddelivery of the message, such as information needed for flow, error control, orcongestion control. The result is the transport-layer packet, which is called the *segment*(in TCP) and the *user datagram* (in UDP). The transport layer then passes thepacket to the network layer.

Figure *Encapsulation/Decapsulation*



3. The network layer takes the transport-layer packet as data or payload and adds itsown header to the payload. The header contains the addresses of the source anddestination hosts and some more information used for error checking of the header,fragmentation information, and so on. The result is the network-layer packet,called a *datagram*. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds itsown header, which contains the link-layer addresses of the host or the next hop (therouter). The result is the link-layer packet, which is called a *frame*. The frame ispassed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connectedto two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates thedatagram from the frame and passes it to the network layer.

2. The network layer only inspects the source and destination addresses in the datagramheader and consults its forwarding table to find the next hop to which the datagram is tobe delivered. The contents of the datagram should not be changed by the network layerin the router unless there is a need to fragment the datagram if it is too big to be passedthrough the next link. The datagram is then passed to the data-link layer of the next link.

3. The data-link layer of the next link encapsulates the datagram in a frame andpasses it to the physical layer for transmission.

Decapsulation at the Destination Host

At the destination host, each layer only decapsulates the packet received, removes thepayload, and delivers the payload to the next-higher layer protocol until the messagereaches the application layer. It is necessary to say that decapsulation in the hostinvolves error checking.

1.5.5 Addressing

It is worth mentioning another concept related to protocol layering in the Internet,*addressing*. As we discussed before, we have logical communication between pairs oflayers in this model. Any communication that involves two parties needs two addresses:source address and destination address. Although it looks as if we need five pairs ofaddresses, one pair per layer, we normally have only four because the physical layer doesnot need addresses; the unit of data exchange at the physical layer is a bit, which definitelycannot have an address. Figure shows the addressing at each layer.As the figure shows, there is a relationship between the layer, the address used inthat layer, and the packet name at that layer. At the application layer, we normally usenames to define the site that provides services, such as *someorg.com*, or the e-mailaddress, such as *somebody@coldmail.com.* At the transport layer, addresses are calledport numbers, and these define the application-layer programs at the source anddestination. Port numbers are local addresses that distinguish between several programsrunning at the same time. At the network-layer, the addresses are global, with the wholeInternet as the scope. A network-layer address uniquely defines the connection of adevice to the Internet. The link-layer addresses, sometimes called MAC addresses, arelocally defined addresses, each of which defines a specific host or router in a network(LAN or WAN). We will come back to these addresses in future chapters.

1.5.6 Multiplexing and Demultiplexing

Since the TCP/IP protocol suite uses several protocols at some layers, we can say that wehave multiplexing at the source and demultiplexing at the destination. Multiplexing in thiscase means that a protocol at a layer can encapsulate a packet from several next-higherlayer protocols (one at a time); demultiplexing means that a protocol can decapsulate anddeliver a packet to several next-higher layer protocols (one at a time). Figure showsthe concept of multiplexing and demultiplexing at the three upper layers.To be able to multiplex and demultiplex, a protocol needs to have a field in itsheader to identify to which protocol the encapsulated packets belong. At the transportlayer, either UDP or TCP can accept a message from several application-layerprotocols. At the network layer, IP can accept a segment from TCP or a user datagramfrom

UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, andso on. At the data-link layer, a frame may carry the payload coming from IP or otherprotocols such as ARP.

Figure *Addressing in the TCP/IP protocol suite*

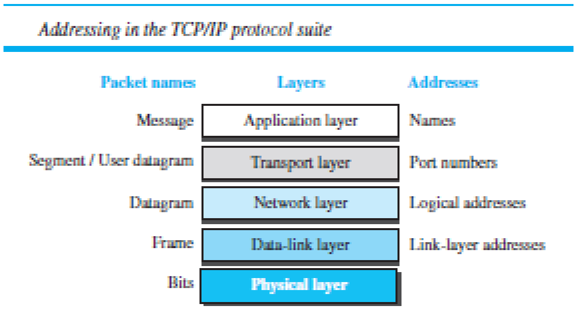
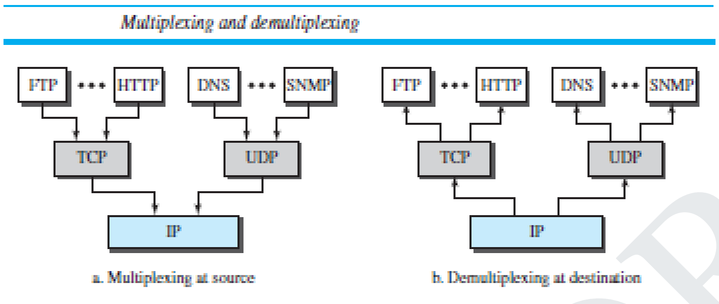


Figure *Multiplexing and demultiplexing*



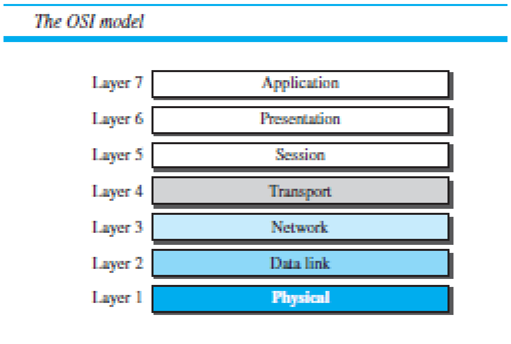
1.6 THE OSI MODEL

Although, when speaking of the Internet, everyone talks about the TCP/IP protocolsuite, this suite is not the only suite of protocols defined. Established in 1947, the**International Organization for Standardization (ISO)** is a multinational bodydedicated to worldwide agreement on international standards. Almost three-fourths ofthe countries in the world are represented in the ISO. An ISO standard that covers allaspects of network communications is the **Open Systems Interconnection (OSI)model.** It was first introduced in the late 1970s.

An *open system* is a set of protocols that allows any two different systems to communicateregardless of their underlying architecture. The purpose of the OSI model isto show how to facilitate communication between different systems without requiringchanges to the logic of the underlying hardware and software. The OSI model is not aprotocol; it is a model for understanding and designing a network architecture that isflexible, robust, and interoperable. The OSI model was intended to be the basis for thecreation of the protocols in the OSI stack.

The OSI model is a layered framework for the design of network systems thatallows communication between all types of computer systems. It consists of seven separatebut related layers, each of which defines a part of the process of moving informationacross a network.

Figure *The OSI model*

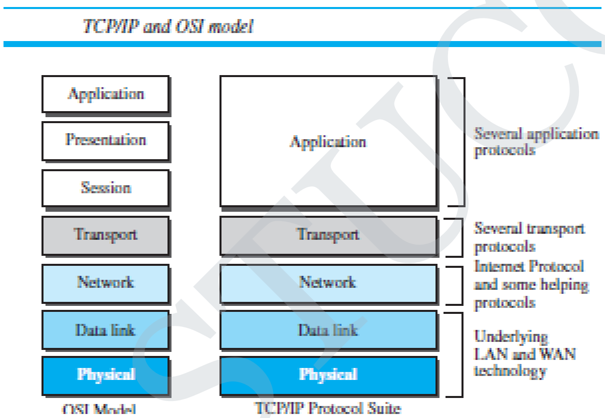


1.6.1 OSI versus TCP/IP

When we compare the two models, we find that two layers, session and presentation,are missing from the TCP/IP protocol suite. These two layers were not added to theTCP/IP protocol suite after the publication of the OSI model. The application layer inthe suite is usually considered to be the combination of three layers in the OSI model.

Two reasons were mentioned for this decision. First, TCP/IP has more than onetransport-layer protocol. Some of the functionalities of the session layer are availablein some of the transport-layer protocols. Second, the application layer is not onlyone piece of software. Many applications can be developed at this layer. If some ofthe functionalities mentioned in the session and presentation layers are needed fora particular application, they can be included in the development of that piece ofsoftware.

Figure *TCP/IP and OSI model*



1.6.2 Lack of OSI Model's Success

The OSI model appeared after the TCP/IP protocol suite. Most experts were at firstexcited and thought that the TCP/IP protocol would be fully replaced by the OSImodel. This did not happen for several reasons, but we describe only three,

First, OSI was completed when TCP/IP wasfully in place and a lot of time and money had been spent on the suite; changing itwould cost a lot.

Second, some layers in the OSI model were never fully defined. Forexample, although the services provided by the presentation and the session layerswere listed in the document, actual protocols for these two layers were not fullydefined, nor were they fully described, and the corresponding software was not fullydeveloped.

Third, when OSI was implemented by an organization in a differentapplication, it did not show a high enough level of performance to entice the Internetauthority to switch from the TCP/IP protocol suite to the OSI model.

1.7 PHYSICAL LAYER:PERFORMANCE

1.7.1 Bandwidth

One characteristic that measures network performance is bandwidth. However, the termcan be used in two different contexts with two different measuring values: bandwidth inhertz and bandwidth in bits per second.

Bandwidth in Hertz

We have discussed this concept. Bandwidth in hertz is the range of frequencies containedin a composite signal or the range of frequencies a channel can pass. For example,bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

The term *bandwidth* can also refer to the number of bits per second that a channel, alink, or even a network can transmit. For example, bandwidth of a FastEthernet network (or the links in this network) is a maximum of 100 Mbps. This meansthat this network can send 100 Mbps.

Relationship

There is an explicit relationship between the bandwidth in hertz and bandwidth in bitsper second. Basically, an increase in bandwidth in hertz means an increase in bandwidthin bits per second. The relationship depends on whether we have baseband transmissionor transmission with modulation.

1.7.2 Throughput

The **throughput** is a measure of how fast we can actually send data through a network.Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bpsthrough this link with *T* always less than *B*. In other words, the bandwidth is a potentialmeasurement of a link; the throughput is an actual measurement of how fast we cansend data. For example, we may have a link with a bandwidth of 1 Mbps, but thedevices connected to the end of the link may handle only 200 kbps. This means that wecannot send more than 200 kbps through this link.

1.7.3 Latency (Delay)

The **latency** or delay defines how long it takes for an entire message to completelyarrive at the destination from the time the first bit is sent out from the source. Latency is made of four components: propagation time, transmission time,queuing time and processing delay.

Latency =propagation time +1 **transmission time** +1 **queuing time +processing delay**

Propagation Time

Propagation time measures the time required for a bit to travel from the source to thedestination. The propagation time is calculated by dividing the distance by the propagationspeed.

Propagation time =**Distance / (Propagation Speed)**

The propagation speed of electromagnetic signals depends on the medium and onthe frequency of the signal. For example, in a vacuum, light is propagated with a speedof 3 × 108 m/s. It is lower in air; it is much lower in cable.

Transmission Time

In data communications we don't send just 1 bit, we send a message. The first bit maytake a time equal to the propagation time to reach its destination; the last bit also maytake the same amount of time. However, there is a time between the first bit leaving thesender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier;the last bit leaves later and arrives later. The **transmission time** of a messagedepends on the size of the message and the bandwidth of the channel.

Transmission time =5 **(Message size) / Bandwidth**

Queuing Time

The third component in latency is the **queuing time**, the time needed for each intermediateor end device to hold the message before it can be processed. The queuing time isnot a fixed factor; it changes with the load imposed on the network. When there isheavy traffic on the network, the queuing time increases. An intermediate device, suchas a router, queues the arrived messages and processes them one by one. If there aremany messages, each message will have to wait.

1.7.4 Bandwidth-Delay Product

Bandwidth and delay are two performance metrics of a link. However, as we will see inthis chapter and future chapters, what is very important in data communications is theproduct of the two, the bandwidth-delay product. Let us elaborate on this issue, usingtwo hypothetical cases as examples.

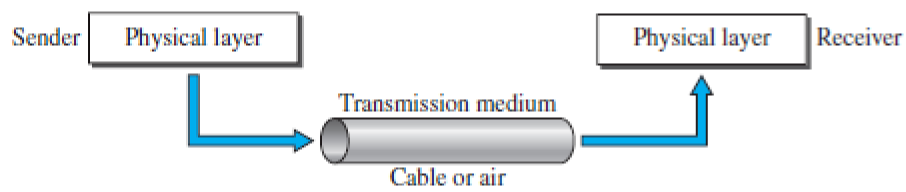
1.7.5 Jitter

Another performance issue that is related to delay is **jitter. J**itteris a problem if different packets of data encounter different delays and the applicationusing the data at the receiver site is time-sensitive (audio and video data, forexample). If the delay for the first packet is 20 ms, for the second is 45 ms, and for thethird is 40 ms, then the real-time application that uses the packets endures jitter.

1.8 TRANSMISSION MEDIA:

Transmission media are actually located below the physical layer and are directly controlledby the physical layer. We could say that transmission media belong to layerzero.

Transmission medium and physical layer



A **transmission medium** can be broadly defined as anything that can carry informationfrom a source to a destination. For example, the transmission medium for twopeople having a dinner conversation is the air. The air can also be used to convey themessage in a smoke signal or semaphore. For a written message, the transmissionmedium might be a mail carrier, a truck, or an airplane.

In data communications the definition of the information and the transmissionmedium is more specific. The transmission medium is usually free space, metallic cable,or fiber-optic cable. The information is usually a signal that is the result of a conversionof data from another form.

The use of long-distance communication using electric signals started with theinvention of the telegraph by Morse in the 19th century. Communication by telegraphwas slow and dependent on a metallic medium.

Extending the range of the human voice became possible when the telephone wasinvented in 1869. Telephone communication at that time also needed a metallic mediumto carry the electric signals that were the result of a conversion from the human voice.

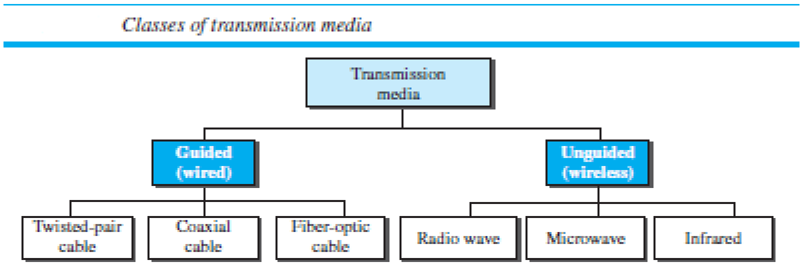
The communication was, however, unreliable due to the poor quality of the wires. Thelines were often noisy and the technology was unsophisticated.Wireless communication started in 1895 when Hertz was able to send highfrequencysignals. Later, Marconi devised a method to send telegraph-type messagesover the Atlantic Ocean.

We have come a long way. Better metallic media have been invented (twisted-pairand coaxial cables, for example). The use of optical fibers has increased the data rateincredibly. Free space (air, vacuum, and water) is used more efficiently, in part dueto the technologies (such as modulation and multiplexing).

Computers and other telecommunication devices usesignals to represent data. These signals are transmitted from one device to another in theform of electromagnetic energy, which is propagated through transmission media.Electromagnetic energy, a combination of electric and magnetic fields vibrating inrelation to each other, includes power, radio waves, infrared light, visible light, ultravioletrays. Each of these constitutes a portion of the **electromagneticspectrum.** In telecommunications, transmission media can be divided into two broad categories:

guided and unguided. Guided media include twisted-pair cable, coaxial cable, andfiber-optic cable. Unguided medium is free space.

Figure *Transmission medium and physical layer*



1.8.1 GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another,include **twisted-pair cable, coaxial cable,** and **fiber-optic cable.** A signal travelingalong any of these media is directed and contained by the physical limits of themedium. Twisted-pair and coaxial cable use metallic (copper) conductors that acceptand transport signals in the form of electric current. **Optical fiber** is a cable that acceptsand transports signals in the form of light.

1.8.1.1 Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plasticinsulation, twisted together, as shown in Figure 7.3.One of the wires is used to carry signals to the receiver, and the other is used onlyas a ground reference. The receiver uses the difference between the two.

In addition to the signal sent by the sender on one of the wires, interference (noise)and crosstalk may affect both wires and create unwanted signals.If the two wires are parallel, the effect of these unwanted signals is not the same inboth wires because they are at different locations relative to the noise or crosstalk sources(e.g., one is closer and the other is farther). This results in a difference at the receiver.

By twisting the pairs, a balance is maintained. For example, suppose in one twist, onewire is closer to the noise source and the other is farther; in the next twist, the reverse istrue. Twisting makes it probable that both wires are equally affected by external influences(noise or crosstalk). This means that the receiver, which calculates the differencebetween the two, receives no unwanted signals. The unwanted signals are mostly canceledout. From the above discussion, it is clear that the number of twists per unit oflength (e.g., inch) has some effect on the quality of the cable.

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as***unshielded twisted-pair*** **(UTP).** IBM has also produced a version of twisted-pair cablefor its use, called

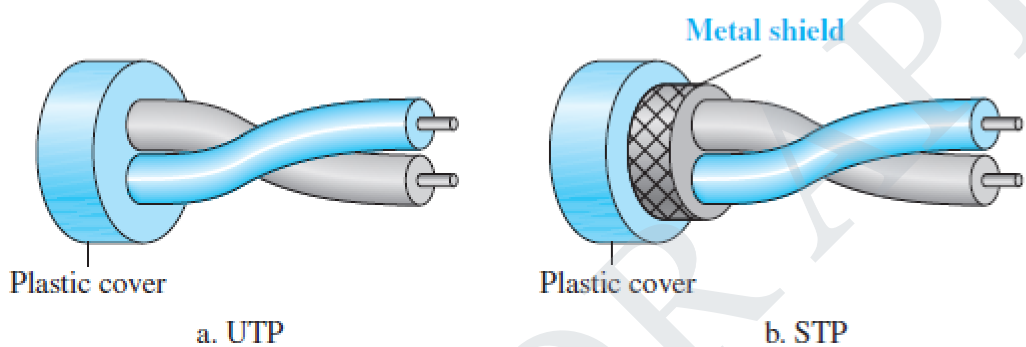
***shielded twisted-pair* (STP).** STP cable has a metal foil or braidedmeshcovering that encases each pair of insulated conductors. Although metal casingimproves the quality of cable by preventing the penetration of noise or crosstalk, it isbulkier and more expensive.

Categories

The Electronic Industries Association (EIA) has developed standards to classifyunshielded twisted-pair cable into seven categories. Categories are determined by cablequality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable forspecific uses. Table 7.1 shows these categories.

Figure *UTP and STP cables*

UTP and STP cables



Connectors

The most common UTP connector is **RJ45** (RJ stands for registered jack), as shownin Figure. The RJ45 is a keyed connector, meaning the connector can be inserted inonly one way.

Performance

One way to measure the performance of twisted-pair cable is to compare attenuationversus frequency and distance. A twisted-pair cable can pass a wide range of frequencies.However, Figure 7.6 shows that with increasing frequency, the attenuation, measured indecibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Notethat ***gauge*** is a measure of the thickness of the wire.

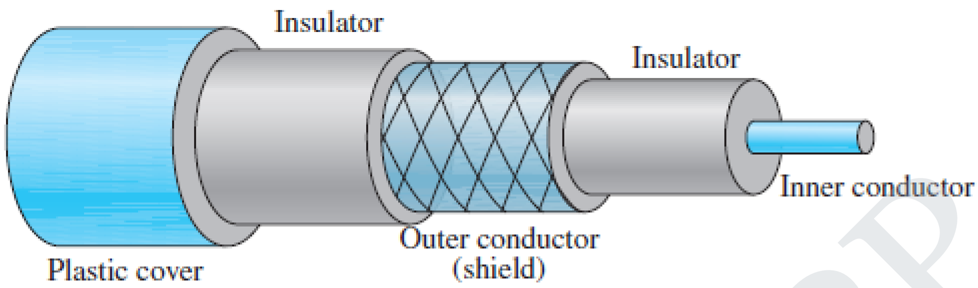
Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels.The local loop—the line that connects subscribers to the central telephone office—commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rateconnections also use the high-bandwidth capability of unshielded twisted-pair cables.

1.8.1.2 Coaxial Cable

Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twistedpaircable, in part because the two media are constructed quite differently. Instead ofhaving two wires, coax has a central core conductor of solid or stranded wire (usuallycopper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductorof metal foil, braid, or a combination of the two. The outer metallic wrapping servesboth as a shield against noise and as the second conductor, which completes the circuit.This outer conductor is also enclosed in an insulating sheath, and the whole cable isprotected by a plastic cover.

Coaxial cable



Coaxial Cable Standards

Coaxial cables are categorized by their **Radio Government (RG)** ratings. Each RGnumber denotes a unique set of physical specifications, including the wire gauge of theinner conductor, the thickness and type of the inner insulator, the construction of theshield, and the size and type of the outer casing.

Coaxial Cable Connectors

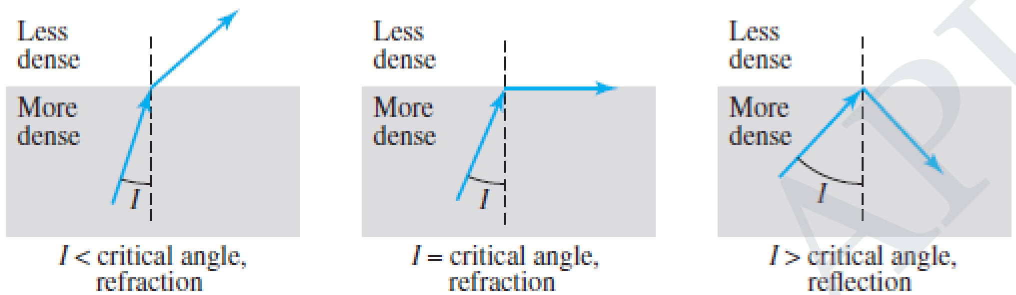
To connect coaxial cable to devices, we need coaxial connectors. The most commontype of connector used today is the **Bayonet Neill-Concelman (BNC)** connector.Figure shows three popular types of these connectors: the BNC connector, theBNC T connector, and the BNC terminator.The BNC connector is used to connect the end of the cable to a device, such as aTV set. The BNC T connector is used in Ethernet networks to branchout to a connection to a computer or other device. The BNC terminator is used at theend of the cable to prevent the reflection of the signal.Cable TV networks (see Chapter 14) also use coaxial cables. In the traditional cableTV network, the entire network used coaxial cable. Later, however, cable TV providersreplaced most of the media with fiber-optic cable; hybrid networks use coaxial cableonly at the network boundaries, near the consumer premises. Cable TV uses RG-59coaxial cable.

Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxialcable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or ThinEthernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbpswith a range of 185 m. The 10Base5, or Thick Ethernet, uses RG-11 (thick coaxial cable)to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors.

1.8.1.3 Fiber-Optic Cable

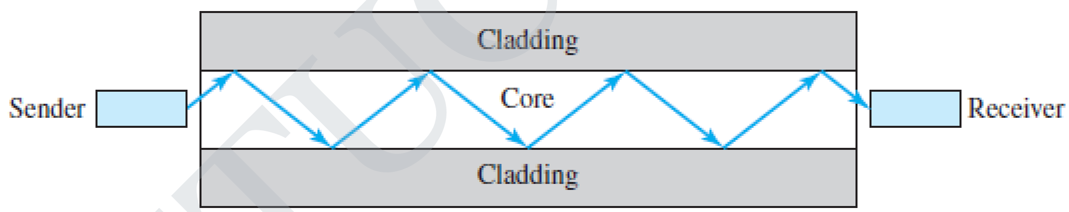
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.To understand optical fiber, we first need to explore several aspects of the nature oflight.Light travels in a straight line as long as it is moving through a single uniform substance.If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction. Figure shows how a ray of lightchanges direction when going from a more dense to a less dense substance.As the figure shows, if the **angle of incidence** *I* (the angle the ray makes with theline perpendicular to the interface between the two substances) is less than the **criticalangle,** the ray **refracts** and moves closer to the surface. If the angle of incidence isequal to the critical angle, the light bends along the interface. If the angle is greater thanthe critical angle, the ray **reflects** (makes a turn) and travels again in the densersubstance. Note that the critical angle is a property of the substance, and its value differsfrom one substance to another.

Bending of light ray



Optical fibers use reflection to guide light through a channel. A glass or plastic **core**is surrounded by a **cladding** of less dense glass or plastic. The difference in density of thetwo materials must be such that a beam of light moving through the core is reflected offthe cladding instead of being refracted into it.

Optical fiber



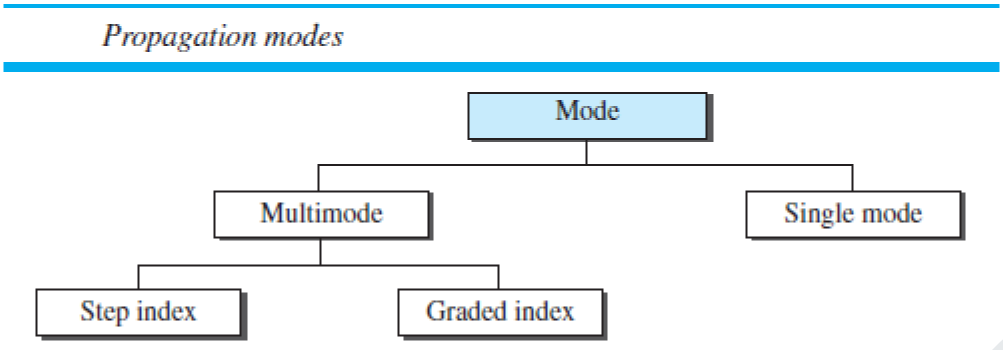
Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating lightalong optical channels, each requiring fiber with different physical characteristics. Multimodecan be implemented in two forms: step-index or graded-index.

Multimode

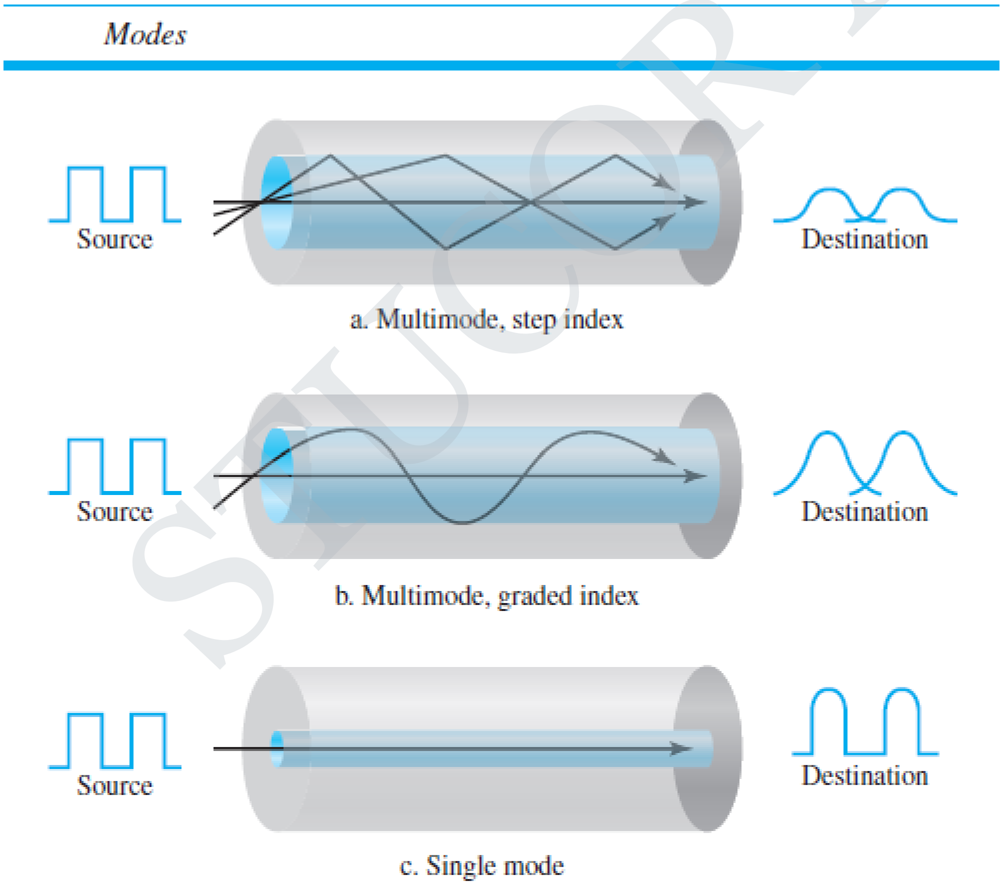
Multimode is so named because multiple beams from a light source move through thecore in different paths. How these beams move within the cable depends on the structureof the core.

Figure *Propagation modes*



In **multimode step-index fiber,** the density of the core remains constant from thecenter to the edges. A beam of light moves through this constant density in a straightline until it reaches the interface of the core and the cladding. At the interface, there isan abrupt change due to a lower density; this alters the angle of the beam's motion. Theterm *step-index* refers to the suddenness of this change, which contributes to the distortionof the signal as it passes through the fiber.

Figure 7.13 *Modes*



A second type of fiber, called **multimode graded-index fiber,** decreases this distortionof the signal through the cable. The word *index* here refers to the index ofrefraction. As we saw above, the index of refraction is related to density. A gradedindexfiber, therefore, is one with varying densities. Density is highest at the center ofthe core and decreases gradually to its lowest at the edge. Figure 7.13 shows the impactof this variable density on the propagation of light beams.

Single-Mode

Single-mode uses step-index fiber and a highly focused source of light that limitsbeams to a small range of angles, all close to the horizontal. The **single-mode fiber**itself is manufactured with a much smaller diameter than that of multimode fiber, andwith substantially lowers density (index of refraction). The decrease in density results ina critical angle that is close enough to 90° to make the propagation of beams almosthorizontal. In this case, propagation of different beams is almost identical, and delaysare negligible. All the beams arrive at the destination "together" and can be recombinedwith little distortion to the signal.

Fiber Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter oftheir cladding, both expressed in micrometers.

Fiber-Optic Cable Connectors

There are three types of connectors for fiber-optic cables. The**subscriber channel (SC) connector** is used for cable TV. It uses a push/pull lockingsystem. The **straight-tip (ST) connector** is used for connecting cable to networkingdevices. It uses a bayonet locking system and is more reliable than SC. **MT-RJ** is aconnector that is the same size as RJ45.

Performance

The plot of attenuation versus wavelength in Figure 7.16 shows a very interestingphenomenon in fiber-optic cable. Attenuation is flatter than in the case of twisted-paircable and coaxial cable. The performance is such that we need fewer (actually onetenthas many) repeaters when we use fiber-optic cable.

Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth iscost-effective. Today, with wavelength-division multiplexing (WDM), we can transferdata at a rate of 1600 Gbps. The SONET network that we discuss in Chapter 14 providessuch a backbone.

Some cable TV companies use a combination of optical fiber and coaxial cable,thus creating a hybrid network. Optical fiber provides the backbone structure whilecoaxial cable provides the connection to the user premises. This is a cost-effective configurationsince the narrow bandwidth requirement at the user end does not justify theuse of optical fiber.

Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-Xalso use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

❑**Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths(and hence data rates) than either twisted-pair or coaxial cable. Currently, data ratesand bandwidth utilization over fiber-optic cable are limited not by the medium butby the signal generation and reception technology available.

❑**Less signal attenuation.** Fiber-optic transmission distance is significantly greaterthan that of other guided media. A signal can run for 50 km without requiringregeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

❑**Immunity to electromagnetic interference.**Electromagnetic noise cannot affectfiber-optic cables.

❑**Resistance to corrosive materials.**Glass is more resistant to corrosive materialsthan copper.

❑**Light weight.**Fiber-optic cables are much lighter than copper cables.

❑**Greater immunity to tapping.**Fiber-optic cables are more immune to tapping thancopper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

❑**Installation and maintenance.**Fiber-optic cable is a relatively new technology. Itsinstallation and maintenance require expertise that is not yet available everywhere.

❑**Unidirectional light propagation.**Propagation of light is unidirectional. If weneed bidirectional communication, two fibers are needed.

❑**Cost.**The cable and the interfaces are relatively more expensive than those of otherguided media. If the demand for bandwidth is not high, often the use of optical fibercannot be justified.

1.8.2 UNGUIDED MEDIA: WIRELESS

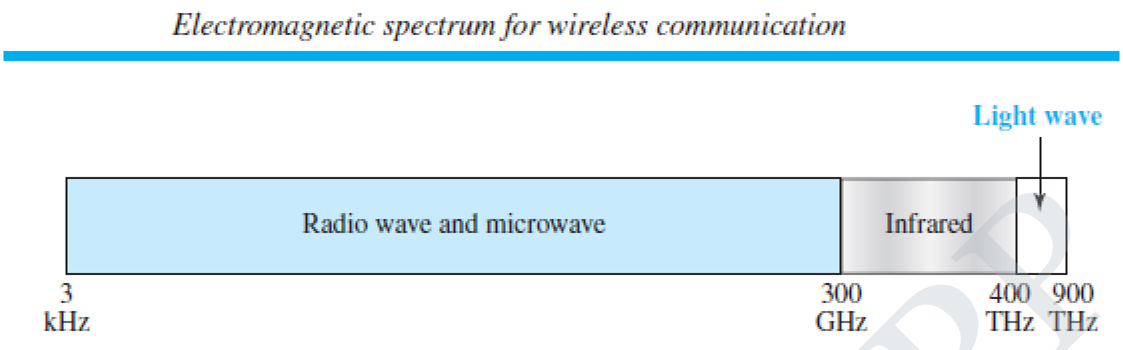
Unguided medium transport electromagnetic waves without using a physical conductor.This type of communication is often referred to as ***wireless communication.*** Signalsare normally broadcast through free space and thus are available to anyone whohas a device capable of receiving them. Figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to900 THz, used for wireless communication.

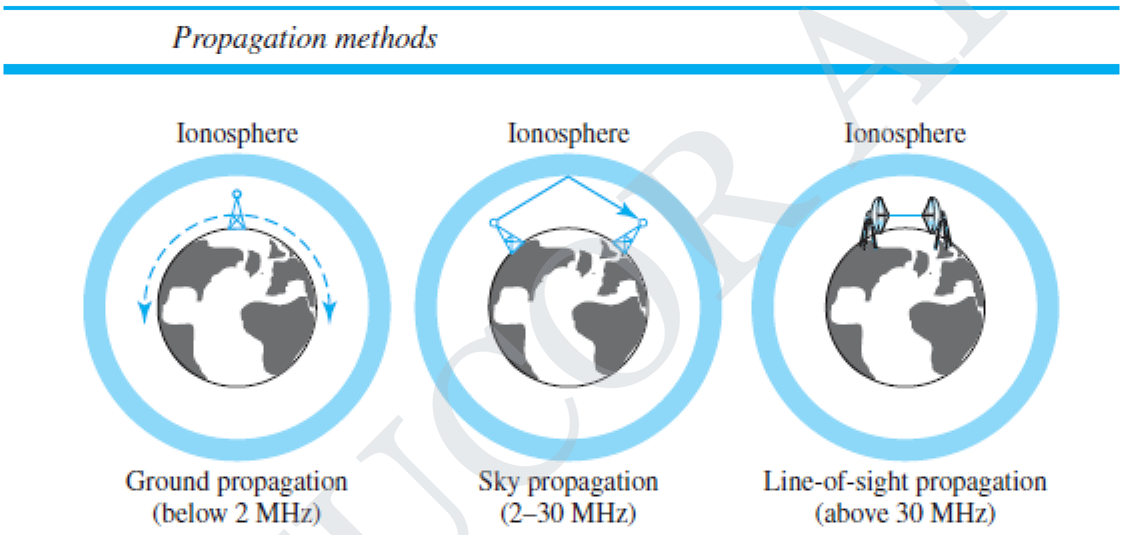
Unguided signals can travel from the source to the destination in several ways: groundpropagation, sky propagation, and line-of-sight propagation.

In **ground propagation,** radio waves travel through the lowest portion of the atmosphere,hugging the earth. These low-frequency signals emanate in all directions from thetransmitting antenna and follow the curvature of the planet. Distance depends on theamount of power in the signal: The greater the power, the greater the distance. In **skypropagation,** higher-frequency radio waves radiate upward into the ionosphere (the layerof atmosphere where particles exist as ions) where they are reflected back to earth. Thistype of transmission allows for greater distances with lower output power.

In **line-of-sightpropagation,** very high-frequency signals are transmitted in straight lines directly fromantenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-ofsightpropagation is tricky because radio transmissions cannot be completely focused.

The section of the electromagnetic spectrum defined as radio waves and microwavesis divided into eight ranges, called *bands,* each regulated by government authorities.These bands are rated from *very low frequency* (VLF) to *extremely high frequency* (EHF).





1.8.2.1 Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagneticwaves ranging in frequencies between 3 kHz and 1 GHz are normally called**radio waves;** waves ranging in frequencies between 1 and 300 GHz are called **microwaves.**However, the behavior of the waves, rather than the frequencies, is a bettercriterion for classification.

Radio waves, for the most part, are omnidirectional. When an antenna transmitsradio waves, they are propagated in all directions. This means that the sending andreceiving antennas do not have to be aligned. A sending antenna sends waves that canbe received by any receiving antenna. The omnidirectional property has a disadvantage,too. The radio waves transmitted by one antenna are susceptible to interference byanother antenna that may send signals using the same frequency or band.Radio waves, particularly those waves that propagate in the sky mode, can travellong distances. This makes radio waves a good candidate for long-distance broadcastingsuch as AM radio.

Radio waves, particularly those of low and medium frequencies, can penetratewalls. This characteristic can be both an advantage and a disadvantage. It is an advantagebecause, for example, an AM radio can receive signals inside a building. It is a disadvantagebecause we cannot isolate a communication to just inside or outside abuilding. The radio wave band is relatively narrow, just under 1 GHz, compared tothe microwave band. When this band is divided into subbands, the subbands are alsonarrow, leading to a low data rate for digital communications.Almost the entire band is regulated by authorities (e.g., the FCC in the United States). Using any part of the band requires permission from the authorities.

Omnidirectional Antenna

Radio waves use **omnidirectional antennas** that send out signals in all directions.Based on the wavelength, strength, and the purpose of transmission, we can have severaltypes of antennas.

Applications

The omnidirectional characteristics of radio waves make them useful for multicasting,in which there is one sender but many receivers. AM and FM radio, television, maritimeradio, cordless phones, and paging are examples of multicasting.

1.8.2.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.Microwaves are unidirectional. When an antenna transmits microwaves, theycan be narrowly focused. This means that the sending and receiving antennas need tobe aligned. The unidirectional property has an obvious advantage. A pair of antennascan be aligned without interfering with another pair of aligned antennas. The followingdescribes some characteristics of microwave propagation:

❑ Microwave propagation is line-of-sight. Since the towers with the mounted antennasneed to be in direct sight of each other, towers that are far apart need to be very tall.The curvature of the earth as well as other blocking obstacles do not allow two shorttowers to communicate by using microwaves. Repeaters are often needed for longdistancecommunication.

❑ Very high-frequency microwaves cannot penetrate walls. This characteristic can bea disadvantage if receivers are inside buildings.

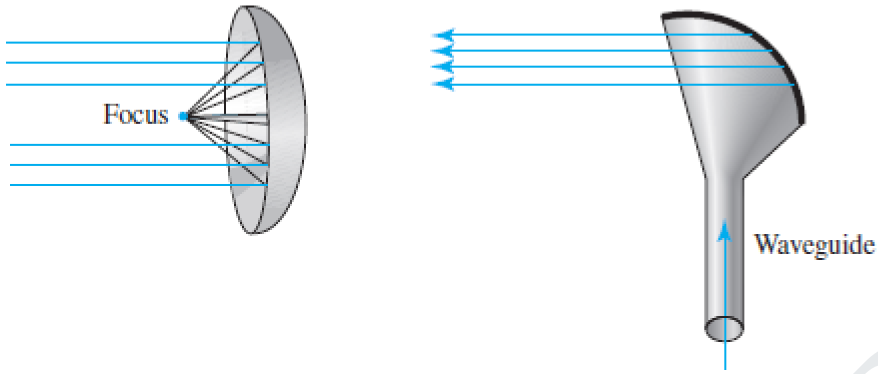
❑The microwave band is relatively wide, almost 299 GHz. Therefore wider subbandscan be assigned, and a high data rate is possible.

❑ Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna

Microwaves need **unidirectional antennas** that send out signals in one direction. Twotypes of antennas are used for microwave communications: the parabolic dish and the horn.

Unidirectional antennas



a. Parabolic dish antenna b. Horn antenna

Radio waves are used for multicast communications,such as radio and television, and paging systems.

A **parabolic dish antenna** is based on the geometry of a parabola: Every lineparallel to the line of symmetry (line of sight) reflects off the curve at angles such thatall the lines intersect in a common point called the focus. The parabolic dish works as afunnel, catching a wide range of waves and directing them to a common point. Inthis way, more of the signal is recovered than would be possible with a single-pointreceiver.

Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaveshit the dish and are deflected outward in a reversal of the receipt path.A **horn antenna** looks like a gigantic scoop. Outgoing transmissions are broadcastup a stem (resembling a handle) and deflected outward in a series of narrow parallelbeams by the curved head. Received transmissions are collected by the scooped shape ofthe horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (oneto-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks, and wireless LANs.

1.8.2.3 Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mmto 770 nm), can be used for short-range communication. Infrared waves, having highfrequencies, cannot penetrate walls. This advantageous characteristic prevents interferencebetween one system and another; a short-range communication system in oneroom cannot be affected by another system in the next room. When we use our infraredremote control, we do not interfere with the use of the remote by our neighbors. However,this same characteristic makes infrared signals useless for long-range communication.In addition, we cannot use infrared waves outside a building because the sun'srays contain infrared waves that can interfere with the communication.

Applications

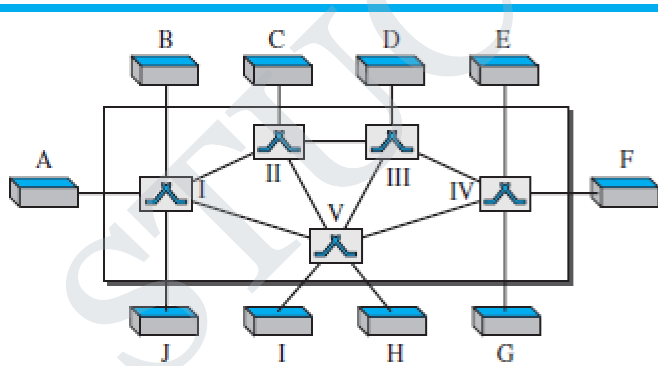
The infrared band, almost 400 THz, has an excellent potential for data transmission.Such a wide bandwidth can be used to transmit digital data with a very high data rate.The *Infrared Data Association* (IrDA), an association for sponsoring the use of infraredwaves, has established standards for using these signals for communication betweendevices such as keyboards, mice, PCs, and printers. For example, some manufacturersprovide a special port called the **IrDA port** that allows a wireless keyboard to communicate with a PC. The standard originally defined a data rate of 75 kbps for a distance up to8 m. The recent standard defines a data rate of 4 Mbps.

1.9 SWITCHING:

A network is a set of connected devices. Whenever we have multiple devices, we havethe problem of how to connect them to make one-to-one communication possible. Onesolution is to make a point-to-point connection between each pair of devices (a meshtopology) or between a central device and every other device (a star topology). Thesemethods, however, are impractical and wasteful when applied to very large networks.The number and length of the links require too much infrastructure to be cost-efficient,and the majority of those links would be idle most of the time. Other topologiesemploying multipoint connections, such as a bus, are ruled out because the distancesbetween devices and the total number of devices increase beyond the capacities of themedia and equipment.

A better solution is switching. A switched network consists of a series of interlinkednodes, called *switches*. Switches are devices capable of creating temporary connectionsbetween two or more devices linked to the switch. In a switched network, some of thesenodes are connected to the end systems (computers or telephones, for example). Othersare used only for routing.

Switched network

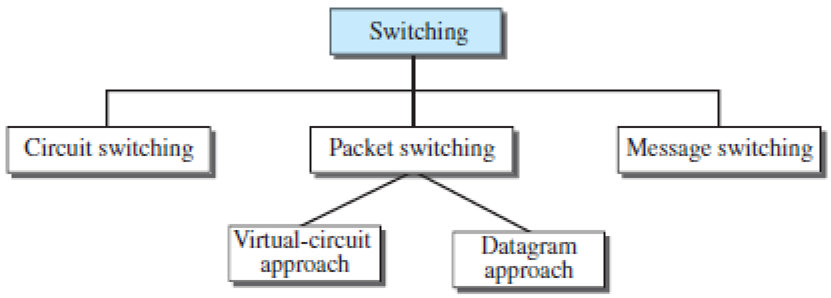


The **end systems** (communicating devices) are labeled A, B, C, D, and so on, and theswitches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

1.9.1 Three Methods of Switching

Traditionally, three methods of switching have been discussed: **circuit switching**,**packet switching**, and **message switching**. The first two are commonly used today.The third has been phased out in general communications but still has networkingapplications. Packet switching can further be divided into two subcategories—virtualcircuit approach and datagram approach.

Taxonomy of switched networks



1.9.2 Switching and TCP/IP Layers

Switching can happen at several layers of the TCP/IP protocol suite.

Switching at Physical Layer

At the physical layer, we can have only circuit switching. There are no packetsexchanged at the physical layer. The switches at the physical layer allow signals totravel in one path or another.

Switching at Data-Link Layer

At the data-link layer, we can have packet switching. However, the term *packet* in thiscase means *frames* or *cells*. Packet switching at the data-link layer is normally doneusing a virtual-circuit approach.

Switching at Network Layer

At the network layer, we can have packet switching. In this case, either a virtual-circuitapproach or a datagram approach can be used. Currently the Internet uses a datagramapproach, but the tendency is to move to a virtual-circuitapproach.

Switching at Application Layer

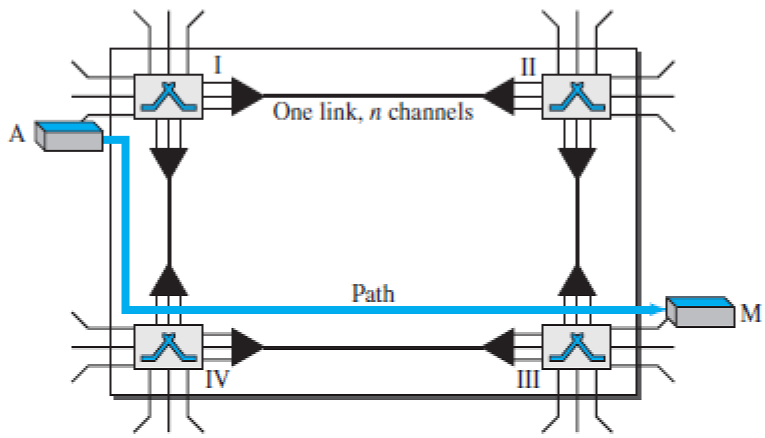
At the application layer, we can have only message switching. The communication atthe application layer occurs by exchanging messages. Conceptually, we can say thatcommunication using e-mail is a kind of message-switched communication, but we donot see any network that actually can be called a message-switched network.

1.10 CIRCUIT-SWITCHED NETWORKS

A **circuit-switched network** consists of a set of switches connected by physical links.A connection between two stations is a dedicated path made of one or more links. However,each connection uses only one dedicated channel on each link. Each link is normallydivided into *n* channels by using FDM or TDM.

Figure shows a trivial circuit-switched network with four switches and fourlinks. Each link is divided into *n* (*n* is 3 in the figure) channels by using FDM or TDM.We have explicitly shown the multiplexing symbols to emphasize the division ofthe link into channels even though multiplexing can be implicitly included in the switchfabric.

A trivial circuit-switched network



The end systems, such as computers or telephones, are directly connected to aswitch. We have shown only two end systems for simplicity. When end system A needsto communicate with end system M, system A needs to request a connection to M thatmust be accepted by all switches as well as by M itself. This is called the **setup phase;**a circuit (channel) is reserved on each link, and the combination of circuits or channelsdefines the dedicated path. After the dedicated path made of connected circuits (channels)is established, the **data-transfer phase** can take place. After all data have been transferred,the circuits are torn down.

We need to emphasize several points here:

❑ Circuit switching takes place at the physical layer.

❑Before starting communication, the stations must make a reservation for the resourcesto be used during the communication. These resources, such as channels (bandwidthin FDM and time slots in TDM), switch buffers, switch processing time, and switchinput/output ports, must remain dedicated during the entire duration of data transferuntil the **teardown phase.**

❑ Data transferred between the two stations are not packetized (physical layer transferof the signal). The data are a continuous flow sent by the source station and receivedby the destination station, although there may be periods of silence.

❑There is no addressing involved during data transfer. The switches route the databased on their occupied band (FDM) or time slot (TDM). Of course, there is end-toendaddressing used during the setup phase.

Three Phases

The actual communication in a circuit-switched network requires three phases: connectionsetup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, adedicated circuit (combination of channels in links) needs to be established. The end systemsare normally connected through dedicated lines to the switches, so connection setupmeans creating dedicated channels between the switches. For example, in Figure,when system A needs to connect to system M, it sends a setup request that includes theaddress of system M, to switch I. Switch I finds a channel between itself and switch IVthat can be dedicated for this purpose. Switch I then sends the request to switch IV,which finds a dedicated channel between itself and switch III. Switch III informs systemM of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needsto be sent in the opposite direction to system A. Only after system A receives thisacknowledgment is the connection established.Note that end-to-end addressing is required for creating a connection between thetwo end systems. These can be, for example, the addresses of the computers assignedby the administrator in a TDM network, or telephone numbers in an FDM network.

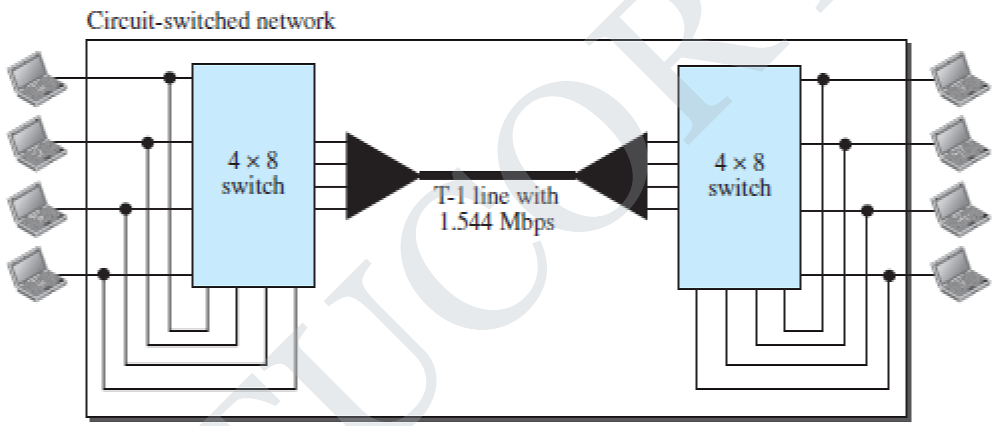
Data-Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to releasethe resources.

Circuit-switched network used in Example 8.2



Efficiency

It can be argued that circuit-switched networks are not as efficient as the other twotypes of networks because resources are allocated during the entire duration of the connection.These resources are unavailable to other connections.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this typeof network is minimal. During data transfer the data are not delayed at each switch; theresources are allocated for the duration of the connection.

1.11 PACKET SWITCHING

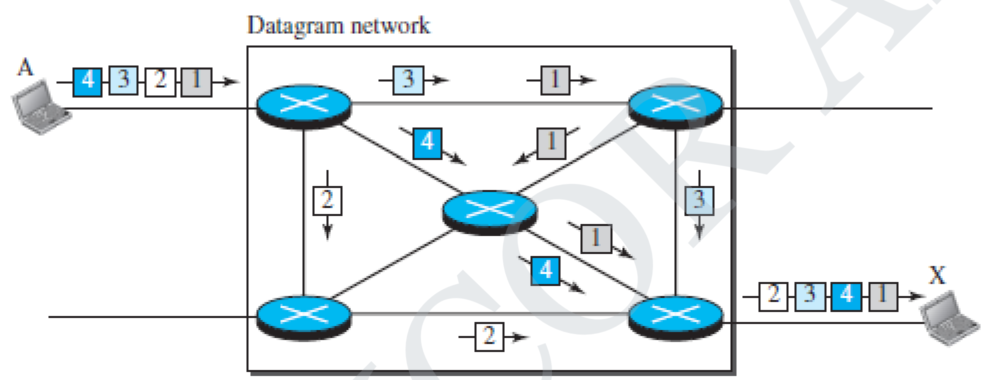
In data communications, we need to send messages from one end system to another. Ifthe message is going to pass through a **packet-switched network**, it needs to bedivided into packets of fixed or variable size. The size of the packet is determined bythe network and the governing protocol.

In packet switching, there is no resource allocation for a packet. This means thatthere is no reserved bandwidth on the links, and there is no scheduled processing timefor each packet. Resources are allocated on demand. The allocation is done on a firstcome,first-served basis. When a switch receives a packet, no matter what the source ordestination is, the packet must wait if there are other packets being processed. As withother systems in our daily life, this lack of reservation may create delay. For example, ifwe do not have a reservation at a restaurant, we might have to wait.

1.11.1 Datagram Networks

In a **datagram network**, each packet is treated independently of all others. Even if apacket is part of a multipacket transmission, the network treats it as though it existedalone. Packets in this approach are referred to as ***datagrams***.

A datagram network with four switches (routers)



All four packets (or datagrams) belong to the same message, butmay travel different paths to reach their destination. This is so because the links may beinvolved in carrying packets from other sources and do not have the necessary bandwidthavailable to carry all the packets from A to X. This approach can cause the datagrams ofa transmission to arrive at their destination out of order with different delays between thepackets. Packets may also be lost or dropped because of a lack of resources. In mostprotocols, it is the responsibility of an upper-layer protocol to reorder the datagrams orask for lost datagrams before passing them on to the application.

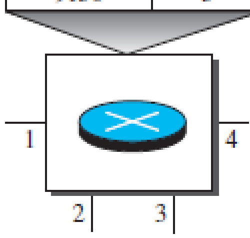
The datagram networks are sometimes referred to as connectionless networks. Theterm connectionless here means that the switch (packet switch) does not keep informationabout the connection state. There are no setup or teardown phases. Each packet is treatedthe same by a switch regardless of its source or destination.

Routing Table

If there are no setup or teardown phases, how are the packets routed to their destinationsin a datagram network? In this type of network, each switch (or packet switch) has a routingtable which is based on the destination address. The routing tables are dynamic andare updated periodically. The destination addresses and the corresponding forwardingoutput ports are recorded in the tables. This is different from the table of a circuitswitchednetwork (discussed later) in which each entry is created when the setup phaseis completed and deleted when the teardown phase is over.Switch in a datagram network uses a routing table that is based on the destinationaddress.

Routing table in a datagram network

Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3



Destination Address

The destination address in the header of a packet in a datagram networkremains the same during the entire journey of the packet.Every packet in a datagram network carries a header that contains, among other information,the destination address of the packet. When the switch receives the packet,this destination address is examined; the routing table is consulted to find the correspondingport through which the packet should be forwarded. This address, unlike theaddress in a virtual-circuit network, remains the same during the entire journey of thepacket.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network;resources are allocated only when there are packets to be transferred. If asource sends a packet and there is a delay of a few minutes before another packet canbe sent, the resources can be reallocated during these minutes for other packets fromother sources.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network.Although there are no setup and teardown phases, each packet may experience a wait at aswitch before it is forwarded. In addition, since not all packets in a message necessarilytravel through the same switches, the delay is not uniform for the packets of a message.

UNIT II DATA-LINK LAYER & MEDIA ACCESS

Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP - Media Access Control - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices.

2.1 Introduction

What is DLL (Data Link Layer)?

The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network. It breaks the datagram passed down by above layers and converts them into frames ready for transfer. This is called **Framing.**

It provides two main functionalities

- Reliable data transfer service between two peer network layers
- Flow Control mechanism which regulates the flow of frames such that data congestion is not there at slow receivers due to fast senders.

2.2 LINK-LAYER ADDRESSING

In a connectionless internetwork such as the Internet we cannot make a datagram reach its destination using only IP addresses. The reason is that each datagram in the Internet, from the same source host to the same destination host, may take a different path. The source and destination IP addresses define the two ends but cannot define which links the datagram should pass through.

Three Types of addresses

Some link-layer protocols define three types of addresses: unicast, multicast, and broadcast.

Unicast Address

Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

A3:34:45:11:92:F1

Multicast Address

Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication. However, the jurisdiction is local (inside the link).

A2:34:45:11:92:F1

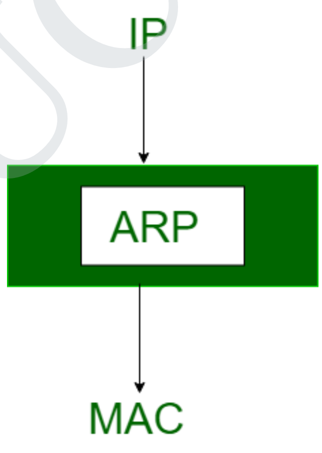
Broadcast Address

Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link. FF:FF:FF:FF:FF:FF

Address Resolution Protocols:

Most of the computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address) i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.

Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.



The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.

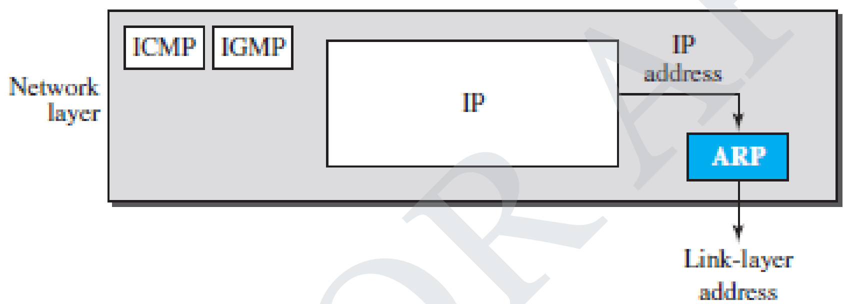
Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

Let's look at how ARP works.

Imagine a device wants to communicate with the other over the internet. What ARP does? Is it broadcast a packet to all the devices of the source network?

The devices of the network peel the header of the data link layer from the protocol data unit (PDU) called frame and transfers the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP's network ID of the packet and if it's equal then it responds to the source with the MAC address of the destination, else the packet reaches the gateway of the network and broadcasts packet to the devices it is connected with and validates their network ID.

Position of ARP in TCP/IP protocol suite

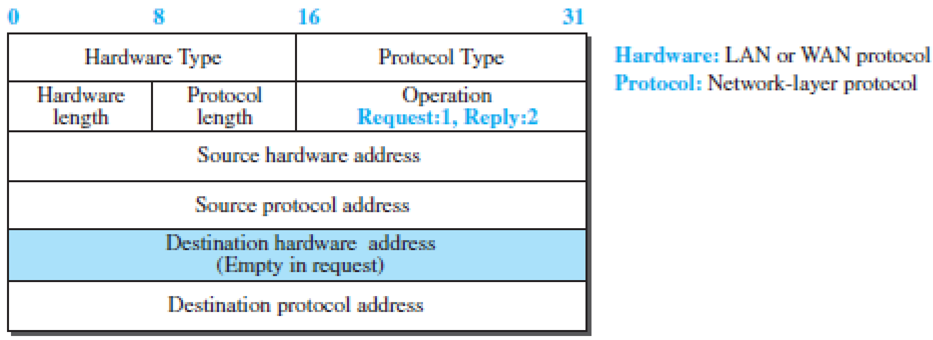


Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address, which we discuss for each protocol later.

Caching

A question that is often asked is this: If system A can broadcast a frame to find the linklayer address of system B, why can't system A send the datagram for system B using a broadcast frame? In other words, instead of sending one broadcast frame (ARP request), one unicast frame (ARP response), and another unicast frame (for sending the datagram), system A can encapsulate the datagram and send it to the network. System B receives it and keep it; other systems discard it.

ARP packet



2.3 DLC Services.

The data link control (DLC) deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast. Data link control functions include framing and flow and error control. In this section, we first discuss framing, or how to organize the bits that are carried by the physical layer. We then discuss flow and error control.

Data link control functions includes

(1) Framing.

(2) Error Control.

(3) Flow Control.

Framing

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing. The data-link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter. In addition, each envelope defines the sender and receiver addresses, which is necessary since the postal system is a manyto- many carrier facility.

Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Although the whole message could be packed in one frame, that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient. When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame. When a message is divided into smaller frames, a single-bit error affects only that small frame.

Frame Size:

Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM WAN, which uses frames of fixed size called cells. Our main discussion in this chapter concerns variable-size framing, prevalent in local-area networks. In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Character-Oriented Framing:

In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits, are also multiples of 8 bits. To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

Bit-Oriented Framing:

In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame.

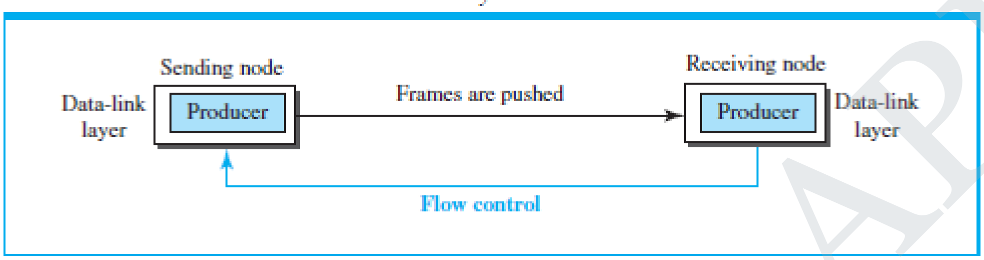
Flow and Error Control

We briefly defined flow and error control in Chapter 9; we elaborate on these two issues here. One of the responsibilities of the data-link control sublayer is flow and error control at the data-link layer.

Flow Control

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates. If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items. If the items are produced more slowly than they can be consumed, the consumer must wait, and the system becomes less efficient. Flow control is related to the first issue. We need to prevent losing the data items at the consumer site. In communication at the data-link layer, we are dealing with four entities: network and data-link layers at the sending node and network and data-link layers at the receiving node. Although we can have a complex relationship with more than one producer and consumer , we ignore the relationships between networks and data-link layers and concentrate on the relationship between two data-link layers.

Flow control at the data-link layer



Buffers

Although flow control can be implemented in several ways, one of the solutions is normally to use two buffers; one at the sending data-link layer and the other at the receiving data-link layer. A buffer is a set of memory locations that can hold packets at the sender and receiver. The flow control communication can occur by sending signals from the consumer to the producer. When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

Error Control:

Since the underlying technology at the physical layer is not fully reliable, we need to implement error control at the data-link layer to prevent the receiving node from delivering corrupted packets to its network layer. Error control at the data-link layer is normally very simple and implemented using one of the following two methods. In both methods, a CRC is added to the frame header by the sender and checked by the receiver.

❑ In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.

❑ In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control) to the sender.

Combination of Flow and Error Control

Flow and error control can be combined. In a simple situation, the acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted. The lack of acknowledgment means that there is a problem in the sent frame. We show this situation when we discuss some simple protocols in the next section. A frame that carries an acknowledgment is normally called an ACK to distinguish it from the data frame.

Connectionless and Connection-Oriented

A DLC protocol can be either connectionless or connection-oriented.

Connectionless Protocol

In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent. Note that the term connectionless here does not mean that there is no physical connection (transmission medium) between the nodes; it means that there is no connection between frames. The frames are not numbered and there is no sense of ordering. Most of the data-link protocols for LANs are connectionless protocols.

Connection-Oriented Protocol

In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase). After all frames that are somehow related to each other are transmitted (transfer phase), the logical connection is terminated (teardown phase). In this type of communication, the frames are numbered and sent in order. If they are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer. Connection oriented protocols are rare in wired LANs, but we can see them in some point-to-point protocols, some wireless LANs, and some WANs.

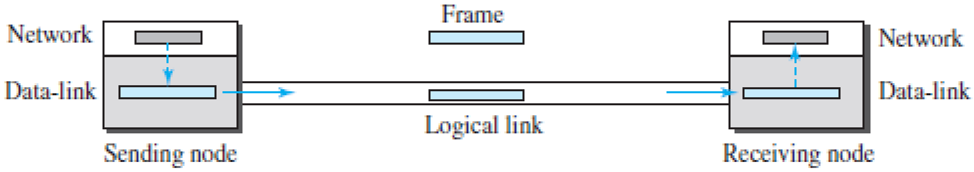
2.4 Data-Link Layer Protocols

Traditionally four protocols have been defined for the data-link layer to deal with flow and error control: Simple, Stop-and-Wait, Go-Back-N, and Selective-Repeat. Although the first two protocols still are used at the data-link layer, the last two have disappeared.

Simple Protocol

Our first protocol is a simple protocol with neither flow nor error control. We assume that the receiver can immediately handle any frame it receives. In other words, the receiver can never be overwhelmed with incoming frames.

Simple protocol



The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame. The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer. The data-link layers of the sender and receiver provide transmission services for their network layers.

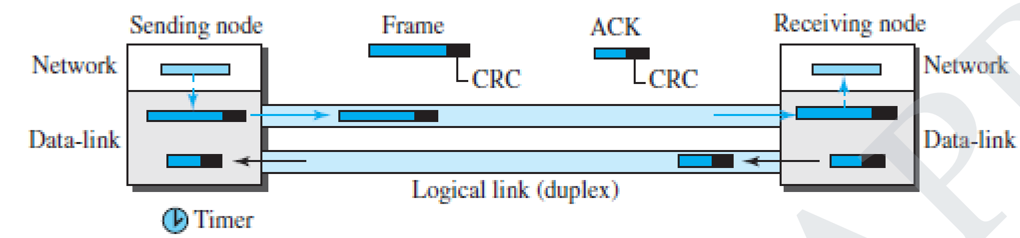
FSMs

The sender site should not send a frame until its network layer has a message to send. The receiver site cannot deliver a message to its network layer until a frame arrives. We can show these requirements using two FSMs. Each FSM has only one state, the ready state. The sending machine remains in the ready state until a request comes from the process in the network layer. When this event occurs, the sending machine encapsulates the message in a frame and sends it to the receiving machine. The receiving machine remains in the ready state until a frame arrives from the sending machine. When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

Stop-and-Wait Protocol

Our second protocol is called the Stop-and-Wait protocol, which uses both flow and error control. We show a primitive version of this protocol here, but we discuss the more sophisticated version in Chapter 23 when we have learned about sliding windows. In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, we need to add a CRC (see Chapter 10) to each data frame. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives. When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.

Stop-and-Wait protocol



Sender States

The sender is initially in the ready state, but it can move between the ready and blocking state.

❑ Ready State. When the sender is in this state, it is only waiting for a packet from the network layer. If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame. The sender then moves to the blocking state.

❑ Blocking State. When the sender is in this state,three events can occur:

a. If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.

b. If a corrupted ACK arrives, it is discarded.

c. If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

Receiver

The receiver is always in the ready state. Two events may occur:

a. If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.

b. If a corrupted frame arrives, the frame is discarded.

Sequence and Acknowledgment Numbers

We saw a problem in Example 11.3 that needs to be addressed and corrected. Duplicate packets, as much as corrupted packets, need to be avoided. As an example, assume we are ordering some item online. If each packet defines the specification of an item to be ordered, duplicate packets mean ordering an item more than once. To correct the problem in Example 11.3, we need to add sequence numbers to the data frames and acknowledgment numbers to the ACK frames. However, numbering in this case is very simple. Sequence numbers are 0, 1, 0, 1, 0, 1, . . . ; the acknowledgment numbers can also be 1, 0, 1, 0, 1, 0, … In other words, the sequence numbers start with 0, the acknowledgment numbers start with 1. An acknowledgment number always defines the sequence number of the next frame to receive.

Piggybacking

The two protocols we discussed in this section are designed for unidirectional communication, in which data is flowing only in one direction although the acknowledgment may travel in the other direction. Protocols have been designed in the past to allow data to flow in both directions. However, to make the communication more efficient, the data in one direction is piggybacked with the acknowledgment in the other direction. In other words, when node A is sending data to node B, Node A also acknowledges the data received from node B. Because piggybacking makes communication at the datalink layer more complicated, it is not a common practice.

2.5 HDLC

HDLC - Short for High-level Data Link Control, a transmission protocol used at the data link layer (layer 2) of the OSI seven layer model for data communications. The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. HDLC is an ISO standard developed from the Synchronous Data Link Control (SDLC) standard proposed by IBM in the 1970's. HDLC NRM (also known as SDLC).

Types of Frames in HDLC

HDLC defines three types of frames:

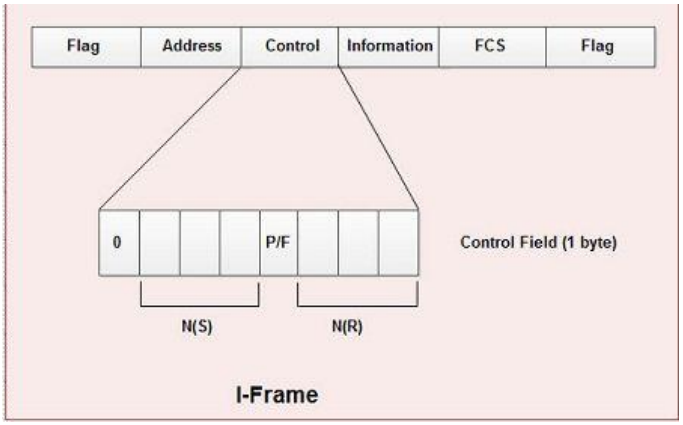
1. Information frames (I-frame)
2. Supervisory frame (S-frame)
3. Unnumbered frame (U-frame)

1. Information frames

• I-frames carry user's data and control information about user's data.

• I-frame carries user data in the information field.

• The I-frame format is shown in diagram.



• The first bit of control field is always zero, *i.e.* the presence of zero at this place indicates that it is I-frame.

• Bit number 2, 3 & 4 in control field is called N(S) that specifies the sequence number of the frame. Thus it specifies the number of the frame that is currently being sent. Since it is a 3.bit field, only eight sequence numbers are possible 0, 1,2,3,4,5,6, 7 (000 to 111).

• Bit number 5 in control field is P/F i.e. Poll/Final and is used for these two purposes. It has, meaning only when it is set i.e. when P/F=1. It can represent the following two cases.

(i) It means poll when frame is sent by a primary station to secondary (when address field contains the address of receiver).

(ii) It means final when frame is sent by secondary to a primary (when the address field contains the address of the sender).

• Bit number 6, 7, and 8 in control field specifies N(R) i.e. the sequence number of the frame expected in return in two-way communication.

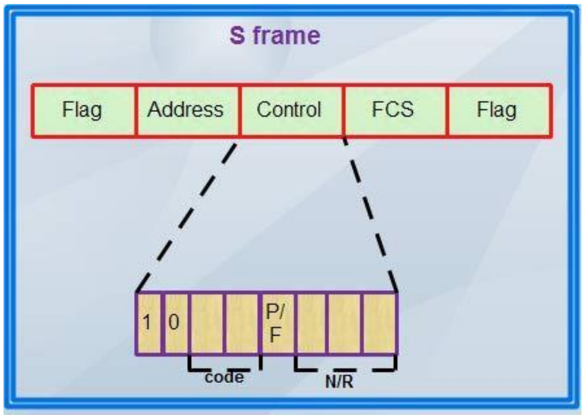
If last frame received was error-free then N(R) number will be that of the next frame is sequence. If the last frame was not received correctly, the N(R) number will be the number of the damaged frame, asking for its retransmission.

2. Supervisory frame

• S-frame carries control information, primarily data link layer flow and error controls.

• It does not contain information field.

• The format of S-frame is shown in diagram.



• The first two bits in the control field of S-frame are always 10.

• Then there is a bit code field that specifies four types of S-frame with combination 00,01, 10, 11 as shown in table :-

Table: Types of S-frame

Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

1. RR, Receive Ready-used to acknowledge frames when no I-frames are availab1e to piggyback the acknowledgement.
2. REJ Reject-used by the receiver to send a NAK when error has occurred.
3. RNR Receive Not Ready-used for flow control.
4. SREJ Selective Reject-indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.

• There is no N(S) field in control field of S-frame as S-frames do not transmit data.

• *P/F* bit is the fifth bit and serves the same purpose as discussed earlier.

• Last three bits in control field indicates N(R) *i.e.* they correspond to the ACK or NAK value.

3. Unnumbered frame

• U-frames are reserved for system management and information carried by them is used for managing the link

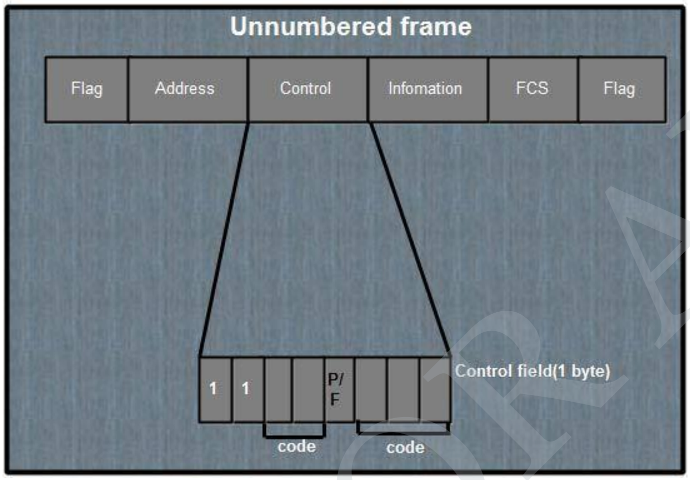
• U-frames are used to exchange session management and control information between the two connected devices.

• Information field in U-frame does not carry user information rather, it carries system management information.

• The frame format of U-frame is shown in diagram.

• U-frame is identified by the presence of 11 in the first and second bit position in control field.

• These frames do not contain N(S) or N(R) in control field.



• U-frame contains two code fields, one two hit and other three bit.

• These five bits can create upto 32 different U-frames.

• .*P/F* bit in control field has same purpose in V-frame as discussed earlier.

Protocol Structure - HDLC: High Level Data Link Control

Flag - The value of the flag is always (0x7E).

Address field - Defines the address of the secondary station which is sending the frame or the destination of the frame sent by the primary station. It contains Service Access Point (6bits), a Command/Response bit to indicate whether the frame relates to information frames (I-frames) being sent from the node or received by the node, and an address extension bit which is usually set to true to indicate that the address is of length one byte. When set to false it indicates an additional byte follows.

Extended address - HDLC provides another type of extension to the basic format. The address field may be extended to more than one byte by agreement between the involved parties.

Control field - Serves to identify the type of the frame. In addition, it includes sequence numbers, control features and error tracking according to the frame type.

FCS - The Frame Check Sequence (FCS) enables a high level of physical error control by allowing the integrity of the transmitted frame data to be checked.

Related Protocols : LAPB , ISDN , X.25 , Frame Relay , SDLC

2.6 POINT-TO-POINT PROTOCOL (PPP)

One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data-link layer. PPP is by far the most common.

Services

The designers of PPP have included several services to make it suitable for a point-to point protocol, but have ignored some traditional services to make it simple.

Services Provided by PPP

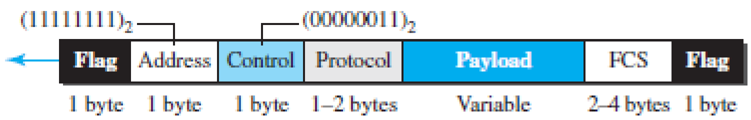
PPP defines the format of the frame to be exchanged between devices. It also defines how two devices can negotiate the establishment of the link and the exchange of data. PPP is designed to accept payloads from several network layers (not only IP). Authentication is also provided in the protocol, but it is optional. The new version of PPP, called Multilink PPP, provides connections over multiple links. One interesting feature of PPP is that it provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

Framing

PPP uses a character-oriented (or byte-oriented) frame. Figure shows the format of a PPP frame. The description of each field follows:

❑ ***Flag.*** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

PPP frame format



❑ ***Address.*** The address field in this protocol is a constant value and set to 11111111 (broadcast address).

❑ ***Control.*** This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection.

❑ ***Protocol.*** The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

❑ ***Payload field.*** This field carries either the user data or other information that we will discuss shortly. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

❑ ***FCS.*** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

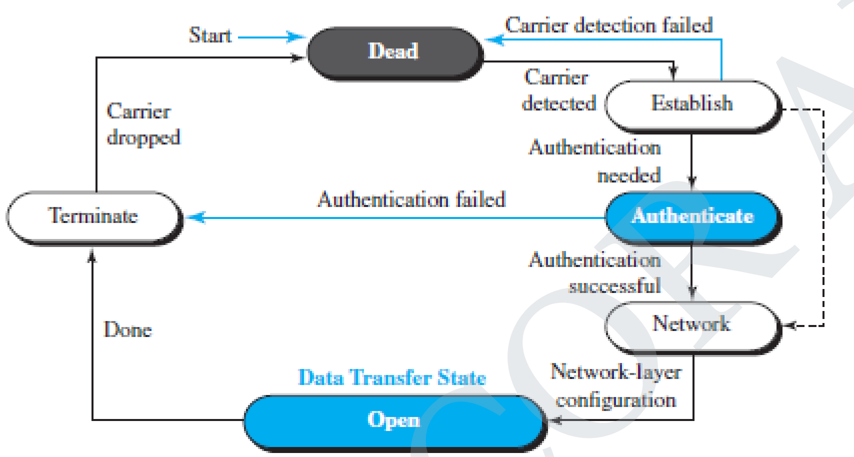
Byte Stuffing

Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101, which means that every time the flaglike pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag. Obviously, the escape byte itself should be stuffed with another escape byte.

Transition Phases

A PPP connection goes through phases which can be shown in a *transition phase* diagram. The transition diagram, which is an FSM, starts with the *dead* state. In this state, there is no active carrier (at the physical layer) and the line is quiet. When one of the two nodes starts the communication, the connection goes into the *establish* state. In this state, options are negotiated between the two parties. If the two parties agree that they need authentication (for example, if they do not know each other), then the system needs to do authentication (an extra step); otherwise, the parties can simply start communication. The link-control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here. Data transfer takes place in the *open* state. When a connection reaches this state, the exchange of data packets can be started. The connection remains in this state until one of the endpoints wants to terminate the connection. In this case, the system goes to the *terminate* state. The system remains in this state until the carrier (physical-layer signal) is dropped, which moves the system to the *dead* state again.

Transition phases



Multiplexing

Although PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate the parties involved, and carry the network-layer data. Three sets of protocols are defined to make PPP powerful: the Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs). At any moment, a PPP packet can carry data from one of these protocols in its data field. Note that there are one LCP, two APs, and several NCPs. Data may also come from several different network layers.

2.7 Media Access Control

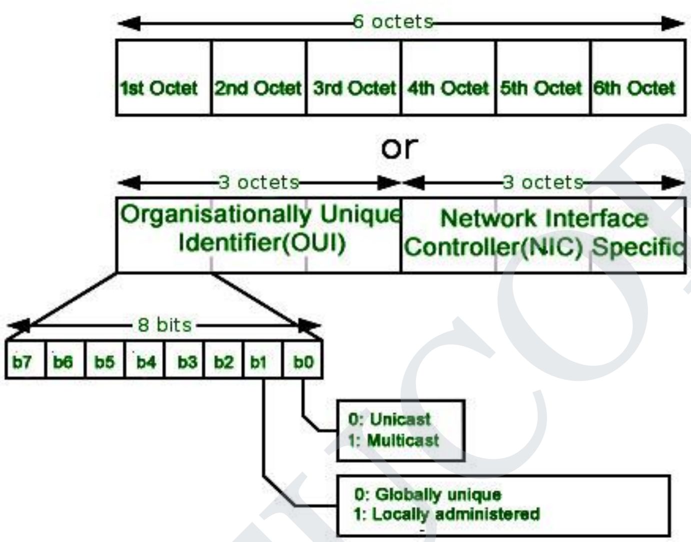
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

Media Access Control (MAC) Address –

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.



Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (Organizational Unique Identifier). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Here are some OUI of well known manufacturers :

CC:46:D6 - Cisco

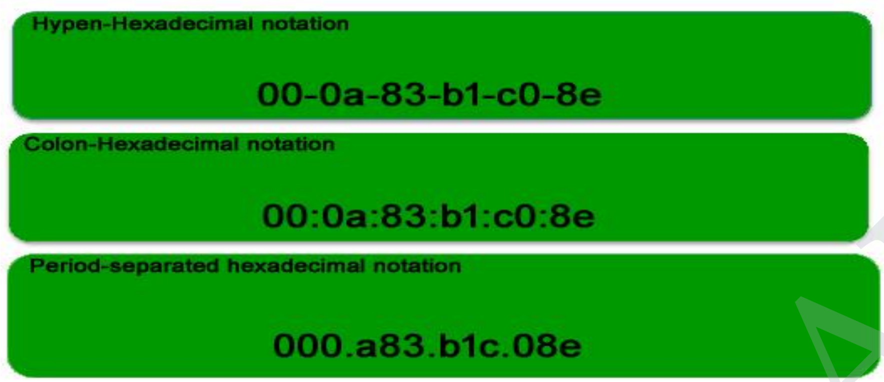
3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represents Network Interface Controller, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



Note: Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

How to find MAC address –

Command for UNIX/Linux - *ifconfig -a*

ip link list

ip address show

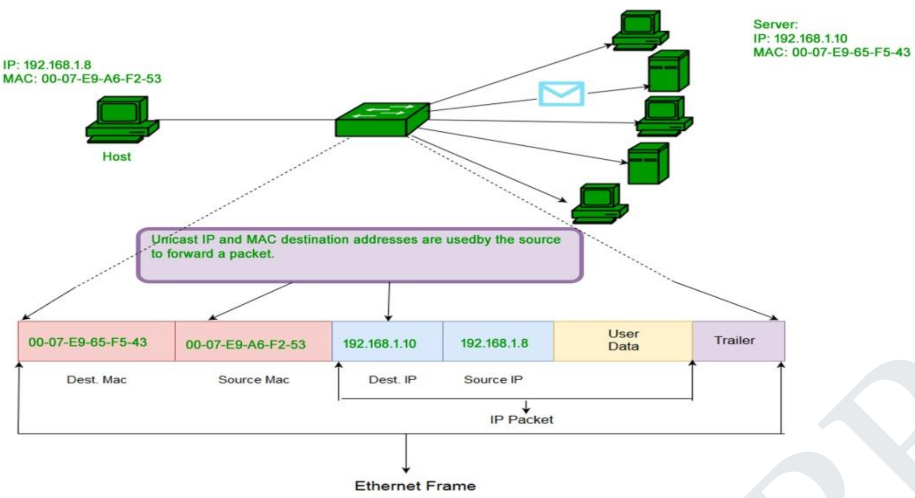
Command forWindows OS - *ipconfig /all*

MacOS - *TCP/IP Control Panel*

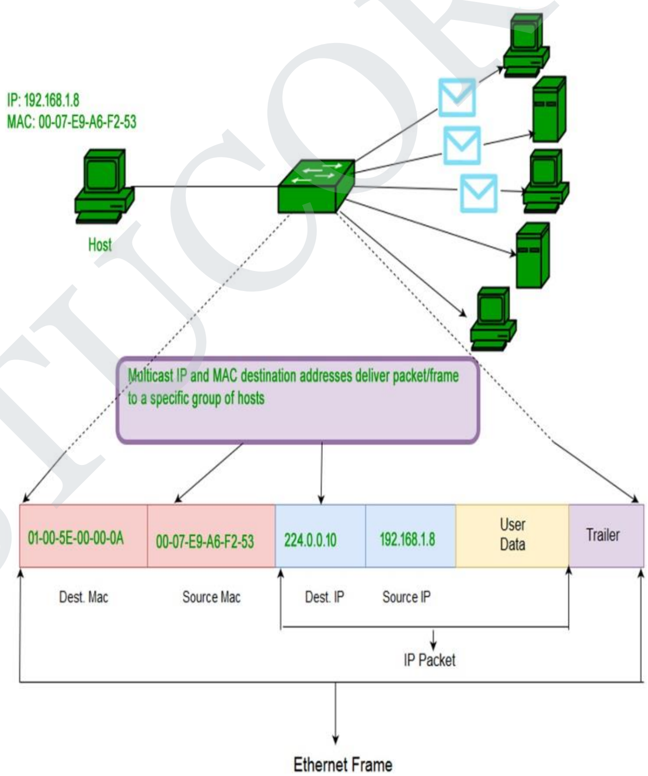
Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

Types of MAC Address –

1. Unicast – A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.

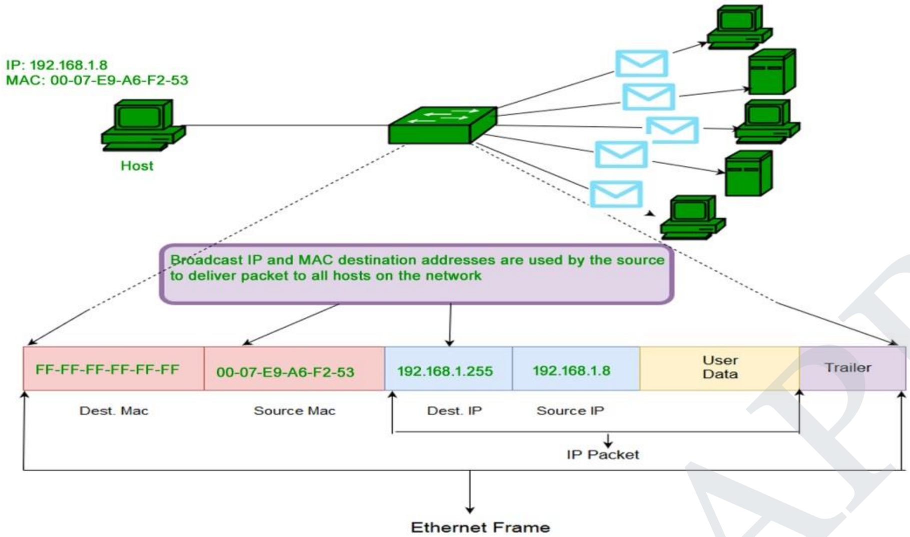


2. **Multicast** – Multicast address allow the source to send a frame to group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



3. **Broadcast** – Similar to Network Layer, Broadcast is also possible on underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-

FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.



What is MAC Cloning –

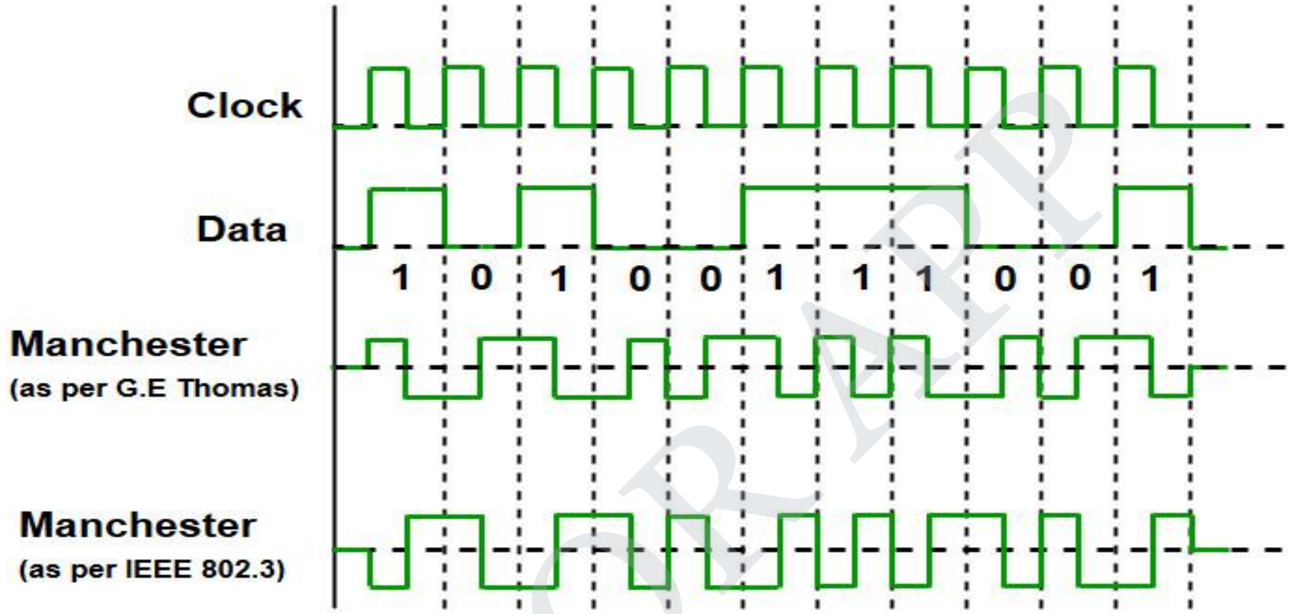
Some ISPs use MAC address inorder to assign IP address to gateway device. When device connects to the ISP, DHCP server records the MAC address and then assign IP address. Now the system will be identified through MAC address. When the device get disconnected, it looses the IP address. If user wants to reconnect, DHCP server checks if the device is connected before. If so, then server tries to assign same IP address (in case lease period not expired). In case user changed the router, user has to inform the ISP about new MAC address because new MAC address is unknown to ISP, so connection cannot be established. Or the other option is Cloning, user can simply clone the registered MAC address with ISP. Now router keeps reporting old MAC address to ISP and there will be no connection issue.

2.8 Wired LANs: Ethernet

Local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection among the devices could be wired or wireless. Ethernet, Token Ring and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.

Ethernet :-

Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies which are allowed. Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD. Manchester Encoding Technique is used in Ethernet.



Since we are talking about IEEE 802.3 standard Ethernet therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and Differential Manchester, Encoding Baud rate is double of bit rate.

Baud rate = 2* Bit rate

Ethernet LANs consist of network nodes and interconnecting media or link. The network nodes can be of two types:

Data Terminal Equipment (DTE):- Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals. DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations. These devices are either the source or the destination of data frames. The data terminal equipment may be a single piece of equipment or multiple pieces of equipment that are interconnected and perform all the required functions to allow the user to communicate. A user can interact to DTE or DTE may be a user.

Data Communication Equipment (DCE):- DCEs are the intermediate network devices that receive and forward frames across the network. They may be either standalone devices such as repeaters, network switches, routers or maybe communications interface units such as interface cards and modems. The DCE performs functions such as signal conversion, coding and may be a part of the DTE or intermediate equipment.

Currently, these data rates are defined for operation over optical fibers and twisted-pair cables:

i) Fast Ethernet

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

ii) Gigabit Ethernet

Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

iii) 10 Gigabit Ethernet

10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s). It is generally used for backbones in high-end applications requiring high data rates.

ALOHA

The Aloha protocol was designed as part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA:

1. Pure Aloha

Pure Aloha is an un-slotted, decentralized, and simple to implement a protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether the channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, the collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects the acknowledgment from the receiver. If it is not received within a specified time, the station assumes that the frame or acknowledgment has been destroyed. Then, the station waits for a random amount of time and sends the frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But in largely loaded networks, this scheme fails poorly. This led to the development of Slotted

Aloha.

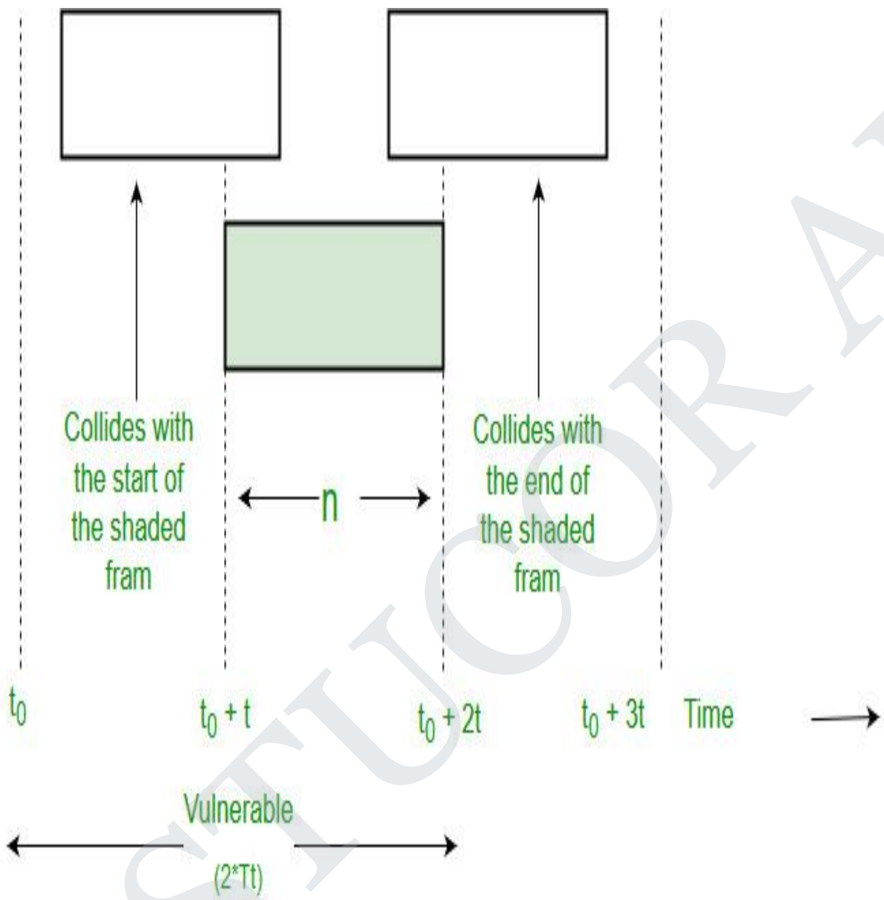
To assure pure aloha: Its throughput and rate of transmission of the frame to be predicted.

For that to make some assumption:

i) All the frames should be the same length.

ii) Stations can not generate frame while transmitting or trying to transmit frame.

iii)The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.



Vulnerable Time = 2 * Tt

Efficiency of Pure ALOHA:

Spure= G * e^-2G

where G is number of stations wants to transmit in Tt slot.

Maximum Efficiency:

Maximum Efficiency will be obtained when G=1/2

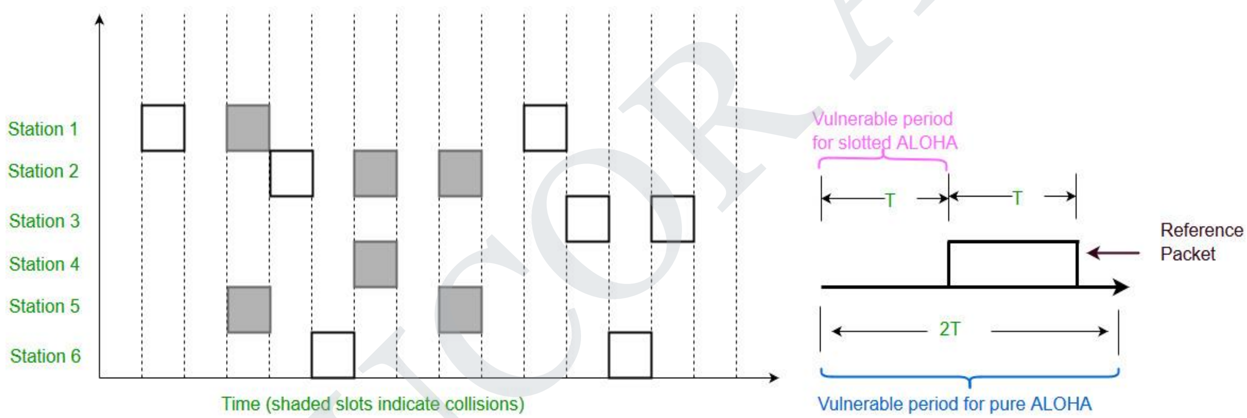
(Spure)*max* = 1/2 * e^-1

= 0.184

Which means, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.

2. Slotted Aloha

This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called *Slots*. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot. But still the number of collisions that can possibly take place is reduced by a large margin and the performance becomes much well compared to Pure Aloha.



Collision is possible for only the current slot. Therefore, Vulnerable Time is Tt.

Efficiency of Slotted ALOHA:

Sslotted = G * e^-G

Maximum Efficiency:

(Sslotted)*max* = 1 * e^-1

= 1/e = 0.368

Maximum Efficiency, in Slotted ALOHA, is 36.8%.

2.9 Wireless LANs- Introduction

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas. Before we discuss a specific protocol related to wireless LANs, let us talk about them in general.

Architectural Comparison

Let us first compare the architecture of wired and wireless LANs to give some idea of what we need to look for when we study wireless LANs.

Medium

The first difference we can see between a wired and a wireless LAN is the medium. In a wired LAN, we use wires to connect hosts. In Chapter 7, we saw that we moved from multiple access to point-to-point access through the generation of the Ethernet. In a switched LAN, with a link-layer switch, the communication between the hosts is point to- point and full-duplex (bidirectional). In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access). In a very rare situation, we may be able to create a point-to-point communication between two wireless hosts by using a very limited bandwidth and two-directional antennas. Our discussion in this chapter, however, is about the multiple-access medium, which means we need to use MAC protocols.

Hosts

In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its network interface card (NIC). Of course, a host can move from one point in the Internet to another point. In this case, its link-layer address remains the same, but its network-layer address will change (Mobile IP section). However, before the host can use the services of the Internet, it needs to be physically connected to the Internet. In a wireless LAN, a host is not physically connected to the network; it can move freely (as we'll see) and can use the services provided by the network.

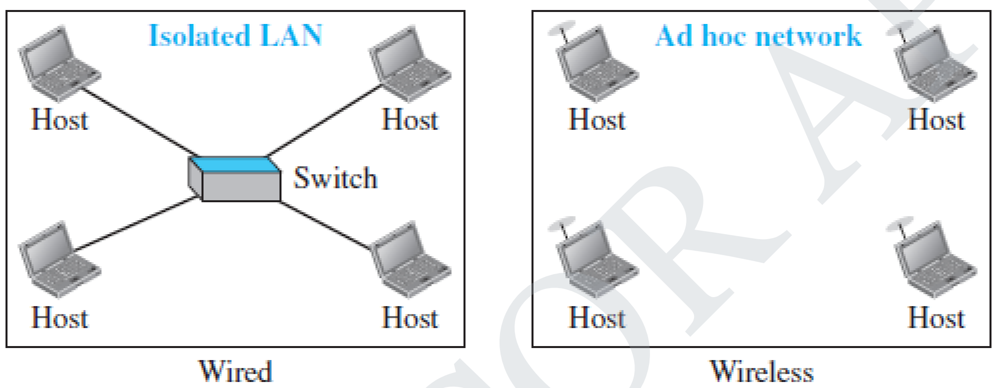
Isolated LANs

The concept of a wired isolated LAN also differs from that of a wireless isolated LAN. A wired isolated LAN is a set of hosts connected via a link-layer switch (in the recent generation of Ethernet). A wireless isolated LAN, called an *ad hoc network* in wireless LAN terminology, is a set of hosts that communicate freely with each other. The concept of a link-layer switch does not exist in wireless LANs. Figure 15.1 shows two isolated LANs, one wired and one wireless.

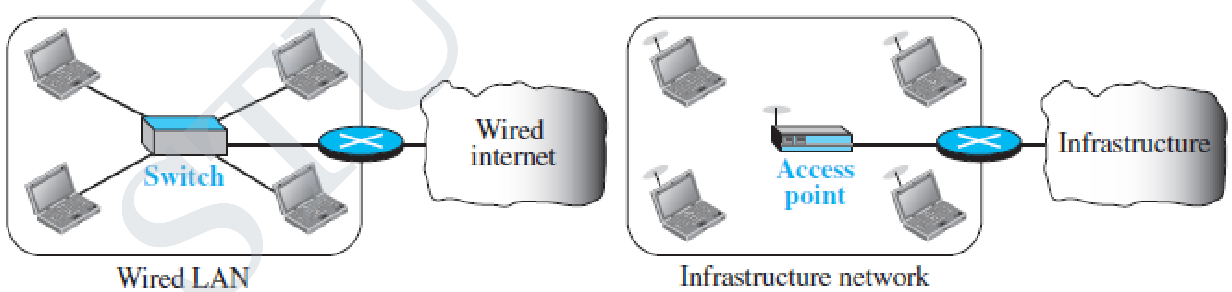
Connection to Other Networks

A wired LAN can be connected to another network or an internetwork such as the Internet using a router. A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN. The first situation is the one that we discuss in this section: connection of a wireless LAN to a wired infrastructure network.

Isolated LANs: wired versus wireless



Connection of a wired LAN and a wireless LAN to other networks



2.10 IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called *wireless Ethernet*. In some countries, including the United States, the public uses the term *WiFi* (short for wireless fidelity) as a synonym for *wireless LAN*. WiFi, however, is a wireless LAN that is certified by the WiFi

Alliance, a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.

Architecture

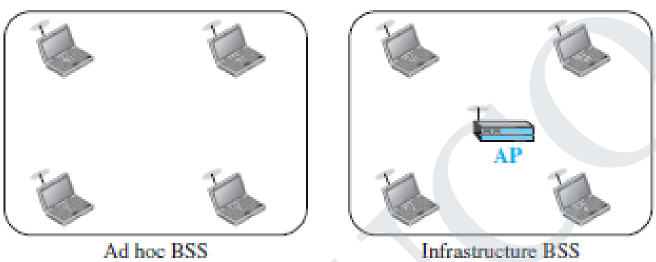
The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*. Figure 15.4 shows two sets in this standard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an *ad hoc architecture*. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an *infrastructure BSS*.

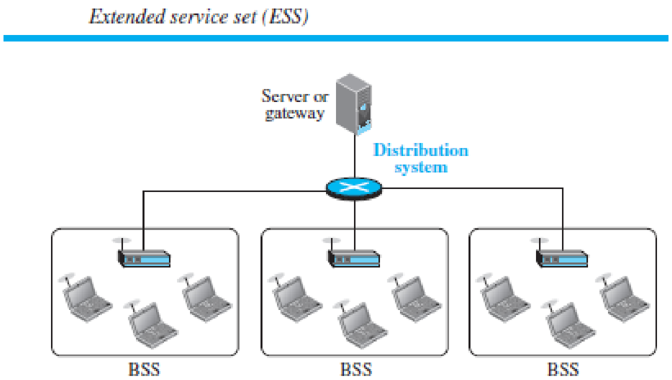
Basic service sets (BSSs)



Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system,* which is a wired or a wireless network. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between a station in a BSS and the outside BSS occurs via the AP. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station.



Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transition, and ESS-transition mobility. A station with **no-transition mobility** is either stationary (not moving) or moving only inside a BSS. A station with **BSS-transition mobility** can move from one BSS to another, but the movement is confined inside one ESS. A station with **ESS-transition mobility** can move from one ESS to another. However, IEEE 802.11 does not guarantee that communication is continuous during the move.

MAC Sublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF). Figure shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.

Distributed Coordination Function

One of the two protocols defined by IEEE at the MAC sublayer is called the ***distributed coordination function (DCF)***. DCF uses CSMA/CA as the access method

Frame Exchange Time Line

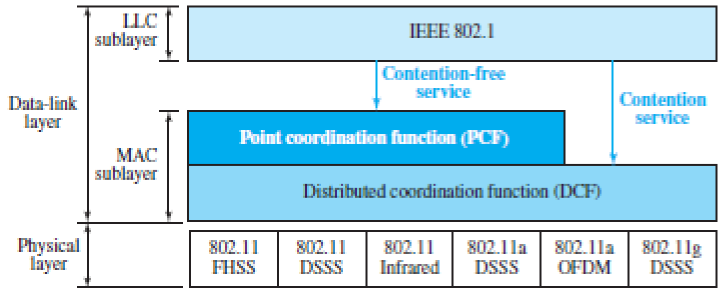
Figure shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with backoff until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the ***distributed interframe space (DIFS);*** then the station sends a control frame called the *request to send (RTS)*.

MAC layers in IEEE 802.11 standard

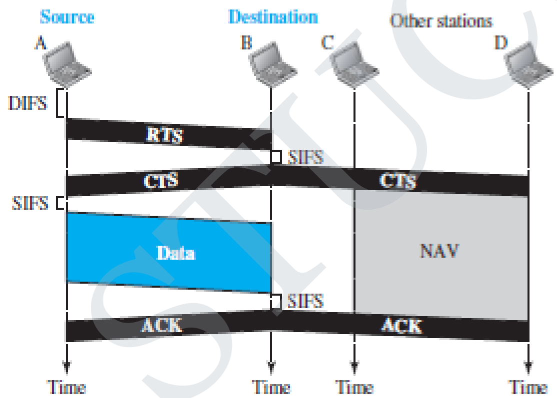


2. After receiving the RTS and waiting a period of time called the ***short interframe space (SIFS),*** the destination station sends a control frame, called the *clear to send (CTS),* to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

CSMA/CA and NAV



Network Allocation Vector

How do other stations defer sending their data if one station acquires access? In other words, how is the *collision avoidance* aspect of this protocol accomplished? The key is a feature called NAV.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a ***network allocation vector (NAV)*** that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired. ***Collision During Handshaking***

What happens if there is a collision during the time when RTS or CTS control frames are in transition, often called the *handshaking period*? Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver. The backoff strategy is employed, and the sender tries again.

Hidden-Station Problem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS). Figure also shows that the RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message, which contains the duration of data ransmission from B to A, reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

2.11 Bluetooth

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

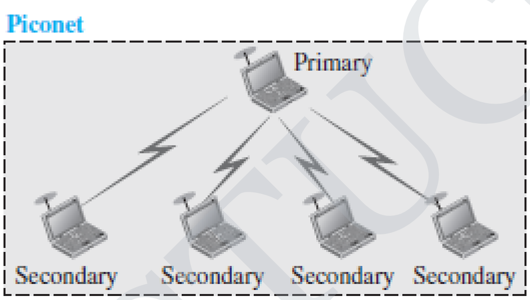
Bluetooth was originally started as a project by the Ericsson Company. It is namedfor Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English. Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

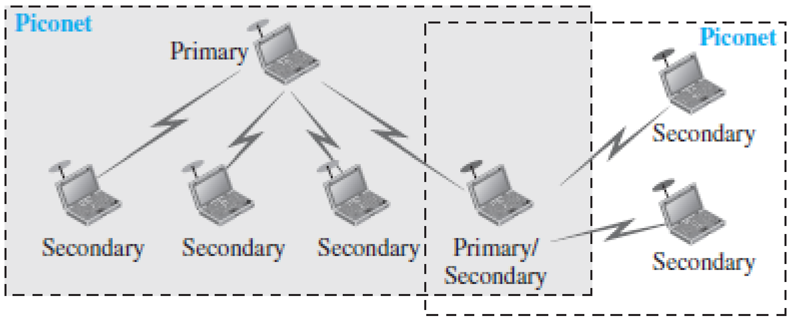
Piconets

A Bluetooth network is called a ***piconet,*** or a small net. A piconet can have up to eight stations, one of which is called the *primary;* the rest are called *secondaries.* All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and secondary stations can be one-to-one or one-to-many. Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state*. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.



Scatternet

Piconets can be combined to form what is called a ***scatternet.*** A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

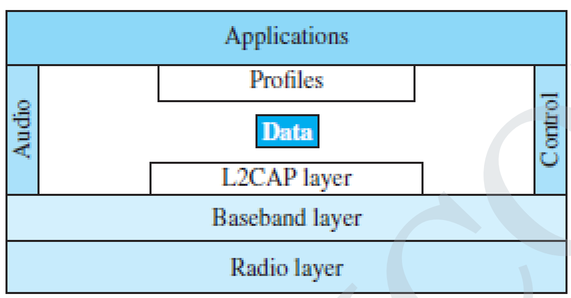


Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

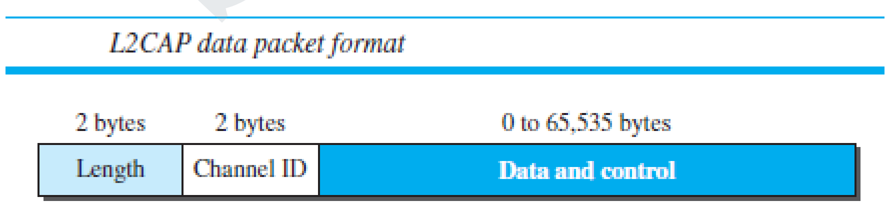
Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet model.



L2CAP

The **Logical Link Control and Adaptation Protocol,** or **L2CAP** (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an The 16-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level.



The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Multiplexing

The L2CAP can do multiplexing. At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

Segmentation and Reassembly

The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes. This includes 4 bytes to define the packet and packet length. Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes. However, application layers sometimes need to send a data packet that can be up to 65,535 bytes (an Internet packet, for example). The L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. The L2CAP segments the packets at the source and reassembles them at the destination.

QoS

Bluetooth allows the stations to define a quality-of-service level. For the moment, it is sufficient to know that if no quality-of-service level is defined, Bluetooth defaults to what is called *best-effort* service; it will do its best under the circumstances.

2.12 Connecting Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from ifferent branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

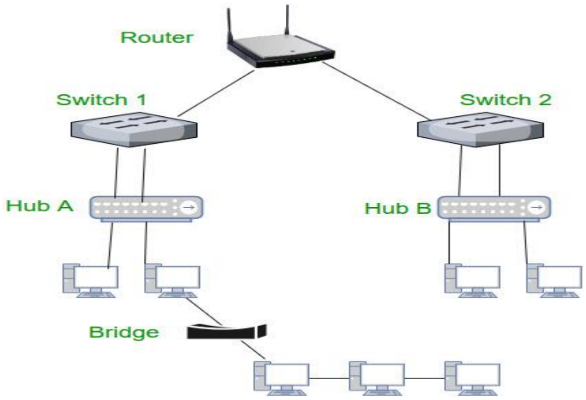
3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges :-** These are the bridge in which the stations are completely naware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges :-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

CS8591 – COMPUTER NETWORKS

UNIT –III

Dr.R.SASIKUMAR
Professor/CSE
R.M.D.Engineering College

NETWORK LAYER

Network Layer

Goals:

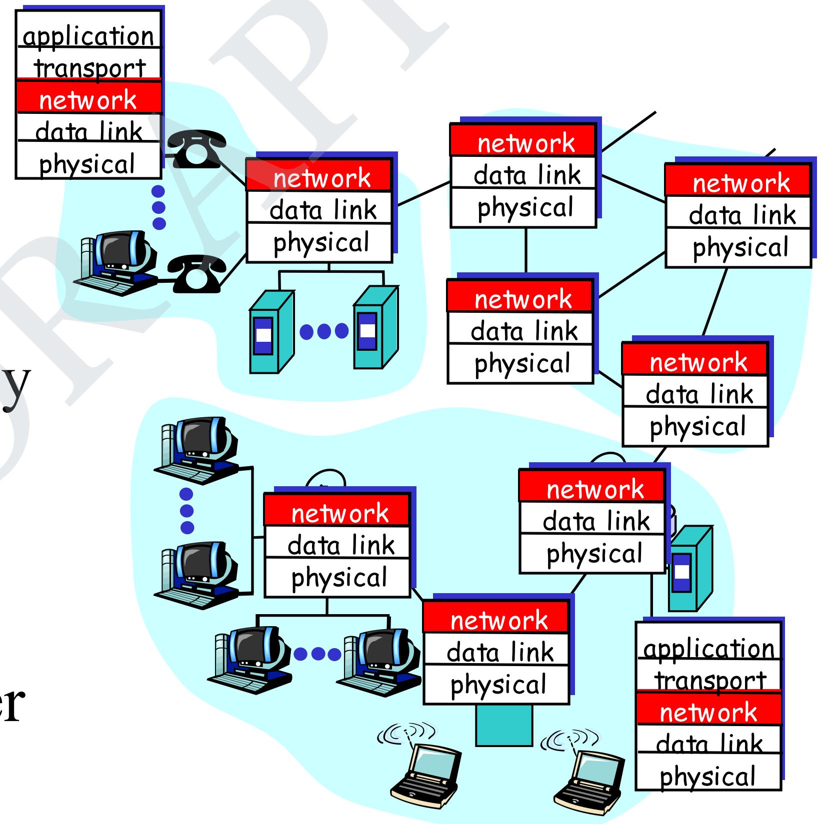
- understand principles behind network layer services:
  - routing (path selection)
  - dealing with scale
  - how a router works
  - advanced topics: IPv6, multicast
- instantiation and implementation in the Internet

Overview:

- network layer services
- routing principle: path selection
- hierarchical routing
- IP
- Internet routing protocols reliable transfer
  - intra-domain
  - inter-domain
- what's inside a router?
- IPv6

Network layer functions

- transport packet from sending to receiving hosts
- network layer protocols in *every* host, router



three important functions:

- *path determination:* route taken by packets from source to dest. *Routing algorithms*
- *switching:* move packets from router's input to appropriate router output
- *call setup:* some network architectures require router call

ath before data flows

Network service model

Q: What *service model* for "channel" transporting packets from sender to receiver?

service abstraction

- guaranteed bandwidth?
- preservation of inter-packet timing (no jitter)?
- loss-free delivery?
- in-order delivery?
- congestion feedback to sender?

The most important abstraction provided by network layer:

virtual circuit
or
datagram?

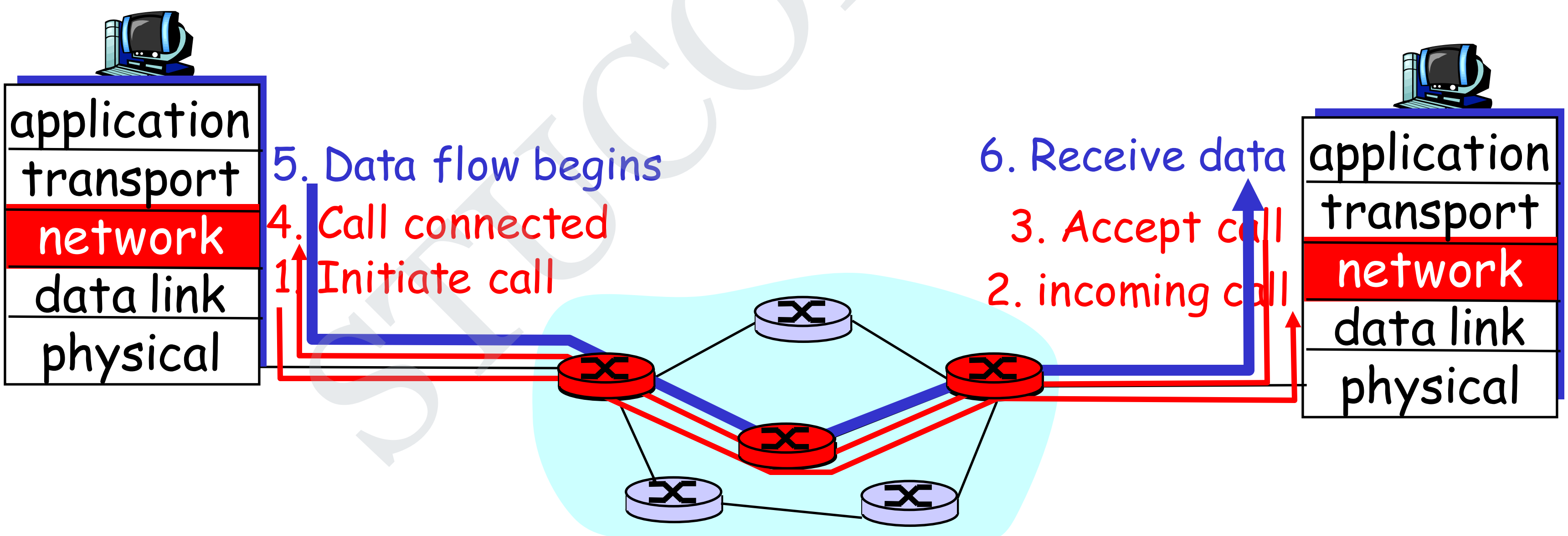
Virtual circuits

"source-to-dest path behaves much like telephone circuit"
- performance-wise
- network actions along source-to-dest path

- call setup, teardown for each call *before* data can flow
- each packet carries VC identifier (not destination host ID)
- *every* router on source-dest path maintains "state" for each passing connection
  - (in contrast, transport-layer connection only involved two end systems)
- link, router resources (bandwidth, buffers) may be *allocated* to VC

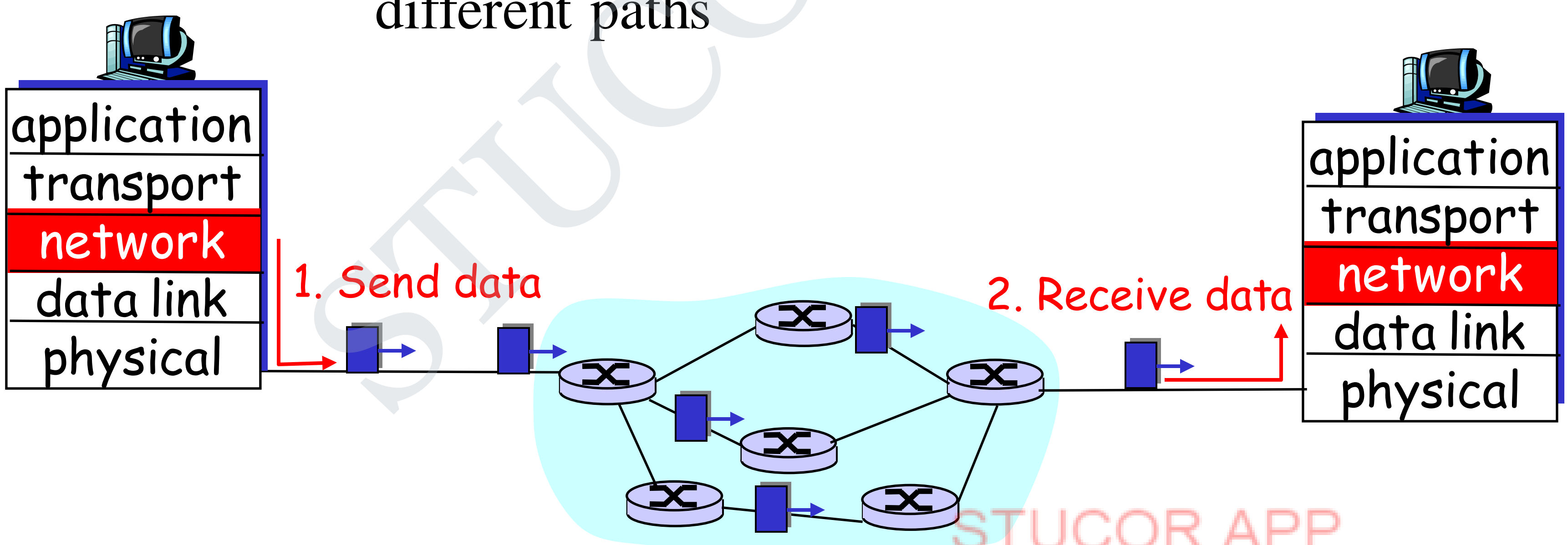
Virtual circuits: signaling protocols

- used to set up, maintain, and tear down VC
- used in ATM, frame-relay, X.25
- not used in today's Internet



Datagram networks: the Internet model

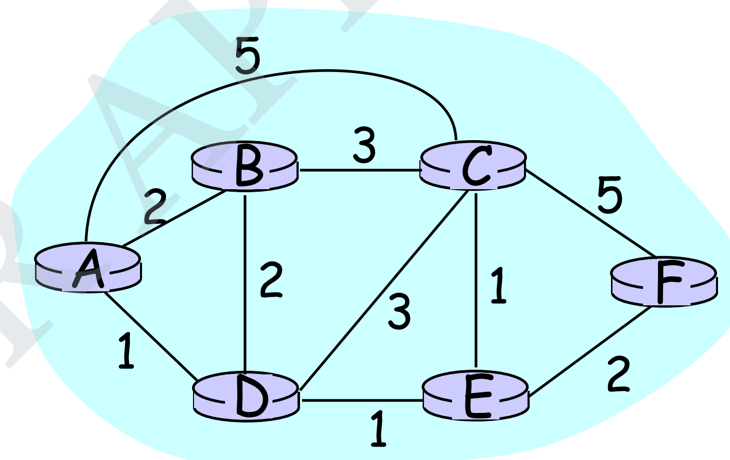
- no call setup at network layer
- routers: no state about end-to-end connections
  - no network-level concept of "connection"
- packets typically routed using destination host ID
  - packets between same source-dest pair may take different paths



Routing

Routing protocol

Goal: determine "good" path (sequence of routers) thru network from source to dest.



Graph abstraction for routing algorithms:

- graph nodes are routers
- graph edges are physical links
  - link cost: delay, $ cost,

- "good" path:
  - typically means minimum cost path
  - other definitions possible

Routing Algorithm classification

Global or decentralized information?

Global:

- all routers have complete topology, link cost info
- "link state" algorithms

Decentralized:

- router knows physically-connected neighbors, link costs to neighbors
- iterative process of computation, exchange of info with neighbors

Static or dynamic?

Static:

- routes change slowly over time (usually by humans)

Dynamic:

- routes change more quickly/automatically
  - periodic update
  - in response to link cost changes

r" algorithms

A Link-State Routing Algorithm

Dijkstra's algorithm

- net topology, link costs known to all nodes
  - accomplished via "link state broadcast"
  - all nodes have same info
- computes least cost paths from one node ('source") to all other nodes
  - gives routing table for that node
- iterative: after k iterations, know least cost path to k

Notation:

- c(i,j): link cost from node i to j. cost infinite if not direct neighbors
- D(v): current value of cost of path from source to dest. V
- p(v): predecessor node along path from source to v, that is next v
- N: set of nodes whose least cost path definitively known

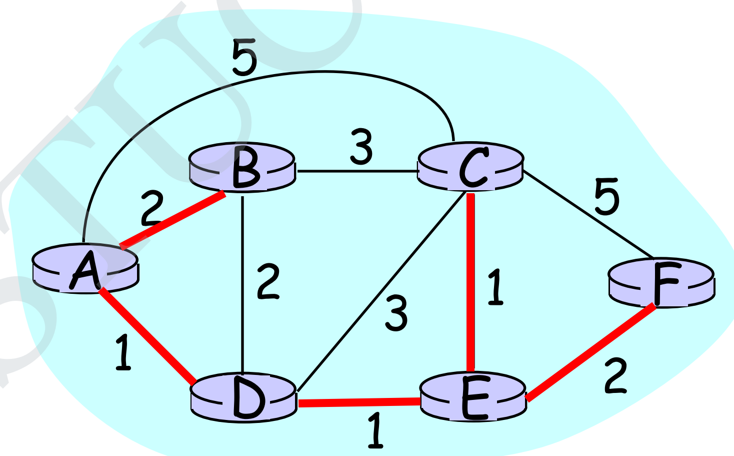
Dijsktra's Algorithm

```
Initialization:
  N = {A}
  for all nodes v
    if v adjacent to A
      then D(v) = c(A,v)
      else D(v) = infty

 Loop
  find w not in N such that D(w) is a minimum (of nodes adjacent to previous w)
   add w to N
   update D(v) for all v adjacent to w and not in N:
      D(v) = min( D(v), D(w) + c(w,v) )
   /* new cost to v is either old cost to v or known
    shortest path cost to w plus cost from w to v */
 until all nodes in N
```

Dijkstra's algorithm: example

Step	start N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	2,A	5,A	1,A	infinity	infinity
1	AD	2,A	4,D		2,D	infinity
2	ADE	2,A	3,E			4,E
3	ADEB		3,E			4,E
4	ADEBC					4,E
5	ADEBCF					



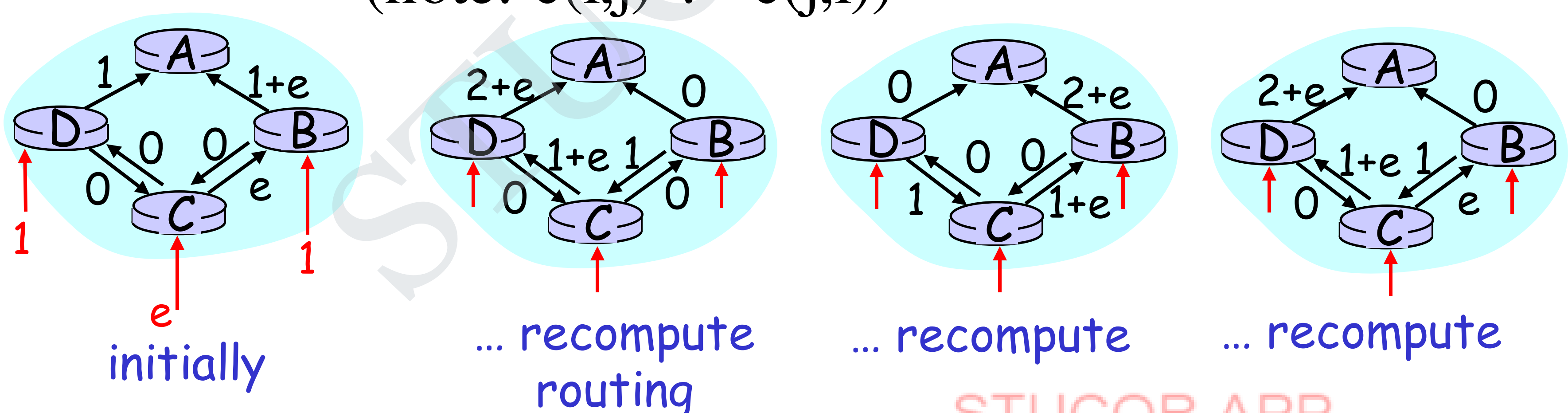
Dijkstra's algorithm, discussion

Algorithm complexity: n nodes

- each iteration: need to check all nodes, w, not in N
- n*(n+1)/2 comparisons: O(n**2)
- more efficient implementations possible: O(nlogn)

Oscillations possible:

- e.g., Suppose link cost = amount of carried traffic (note: c(i,j) != c(j,i))



IPv4 Address

- The IPv4 addresses are unique and universal.
- An IPv4 address is 32 bits long.
  - The address space of IPv4 is 2^{32} (4,294,967,296)
  - Notation.
    - Binary notation
    - Dotted-decimal notation

10000000 00001011 00000011 00011111

128.11.3.31

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent (see Appendix B).

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 19.3

Find the error, if any, in the following IPv4

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. ***There must be no leading zero (045).***

b. ***There can be no more than four numbers.***

c. ***Each number needs to be less than or equal to 255.***

d. ***A mixture of binary notation and dotted-decimal***

Classful Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Find the class of each address.

a. **<u>0</u>**0000001 00001011 00001011 11101111

b. **<u>110</u>**00001 10000011 00011011 11111111

c. **<u>14</u>**.23.120.8

d. **<u>252</u>**.5.15.111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14; the class is A.

Classes and Blocks

- The classful addressing wastes a large part of the address space.
  - Class A:
  - Class B:
  - Class C:
  - Class D:

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Structure of IPv4 Address

- Consists of Net ID and Host ID.

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- Mask
  - 32-bit number of contiguous 1's followed by contiguous 0's.
  - To help to find the net ID and the host ID.

Use of IPv4 Address

- Subnetting
  - Divide a large address block into smaller sub-groups.
  - Use of flexible net mask.
- Supernetting
  - Exhausted class A and B address space
  - Huge demand for class B address space
  - To combine several contiguous address spaces into a larger single address space

Classless Addressing

- To overcome the depletion of address space.
- Restriction
  - The addresses in a block must be contiguous.
  - The number of addresses in a block must be a power of 2.
  - The first address must be evenly divisible by the number of address.
- Mask
  - Consists of *n* consecutive 1's followed by zeros.
  - *n* can be any number b/w 0 and 32.
- Tips:
  - In IPv4 addressing, a block of addresses can be defined as x.y.z.t /n, in which x.y.z.t defines one of the addresses and the /n defines the mask.
  - The first address in the block can be found by setting the rightmost 32 − n bits to 0s.
  - The last address in the block can be found by setting the rightmost 32 − n bits to 1s.
  - The number of addresses in the block can be found by using the formula 2^{32-n}.

Special Addresses

- Network address
  - The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.
- Broadcast address
  - The last address in a block is used for broadcasting to all devices under the network.

Routing in IPv4

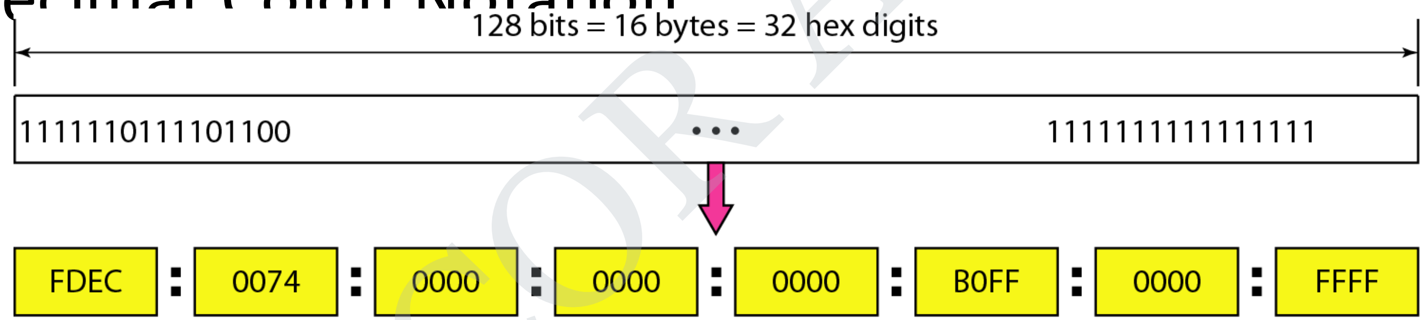
- A router has two addresses
  - An address through which the device inside of the router can be accessed.
  - Another address belongs to the granted block (sub-network).

Hierarchy of IPv4 Addressing

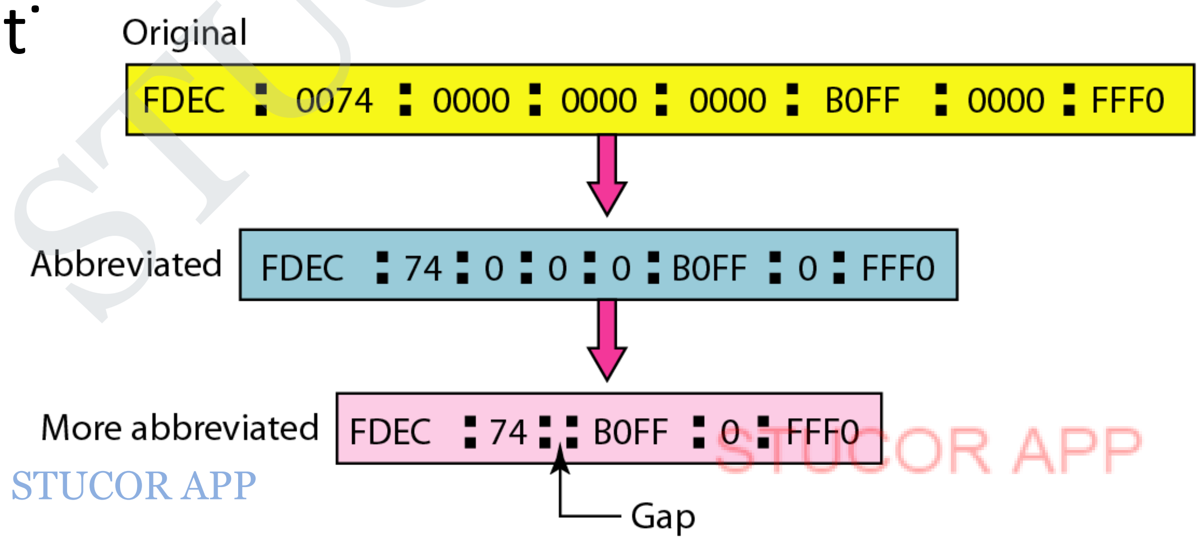
- Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define
  the network; the rightmost 32 − *n* bits define the host.
- Why Hierarchy?

IPv6 Address

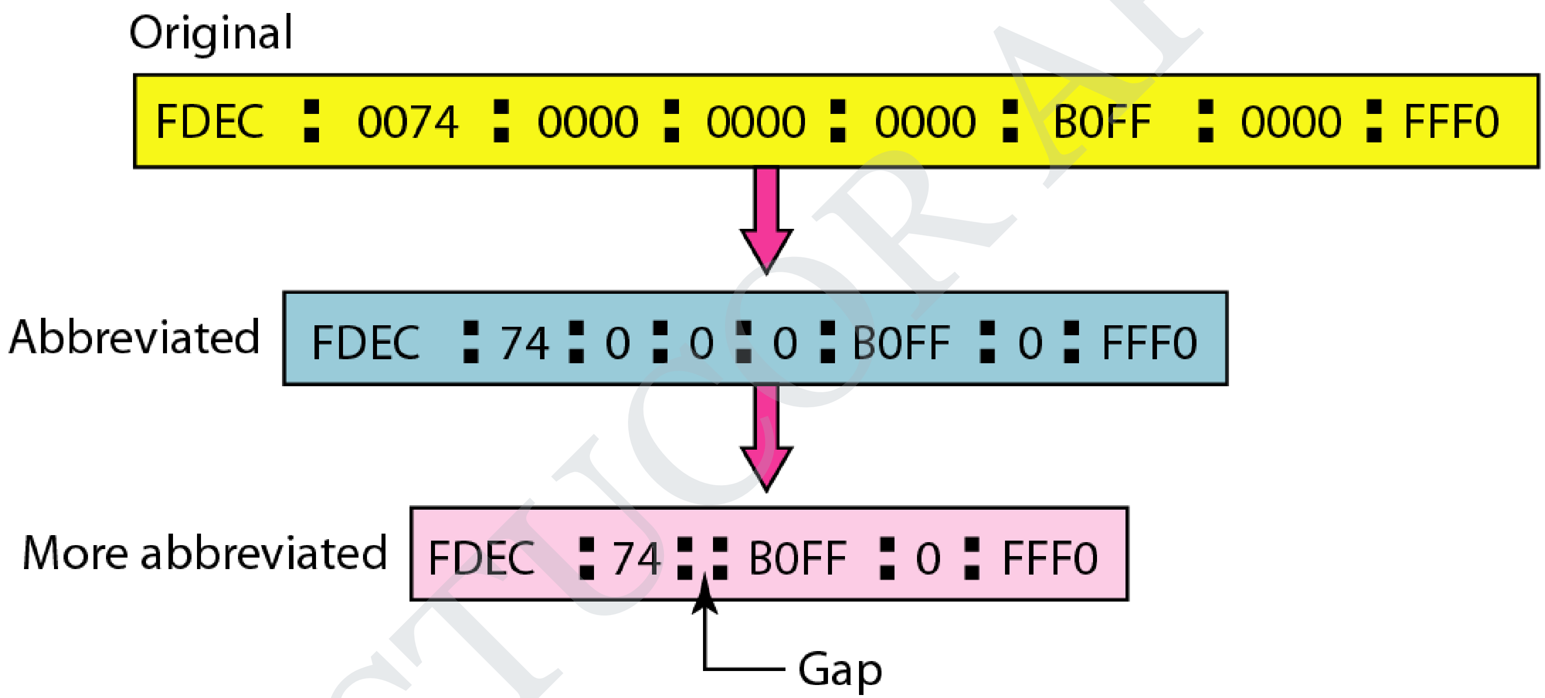
- An IPv6 address is 128 bits long (16-byte).
- Hexadecimal Colon Notation



- Abbreviat



Abbreviated IPv6 addresses



Expand the address 0:15::1:12:1213 to its original.

Solution

We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
   0:  15:                 :   1:  12:1213
```

This means that the original address is.

```
0000:0015:0000:0000:0000:0001:0012:1213
```

Structure of IPv6 Address

- Type prefix
  - For categorization,
  - Variable length,
  - No partial conflict among the different prefix
  -

Type prefixes for IPv6 addresses

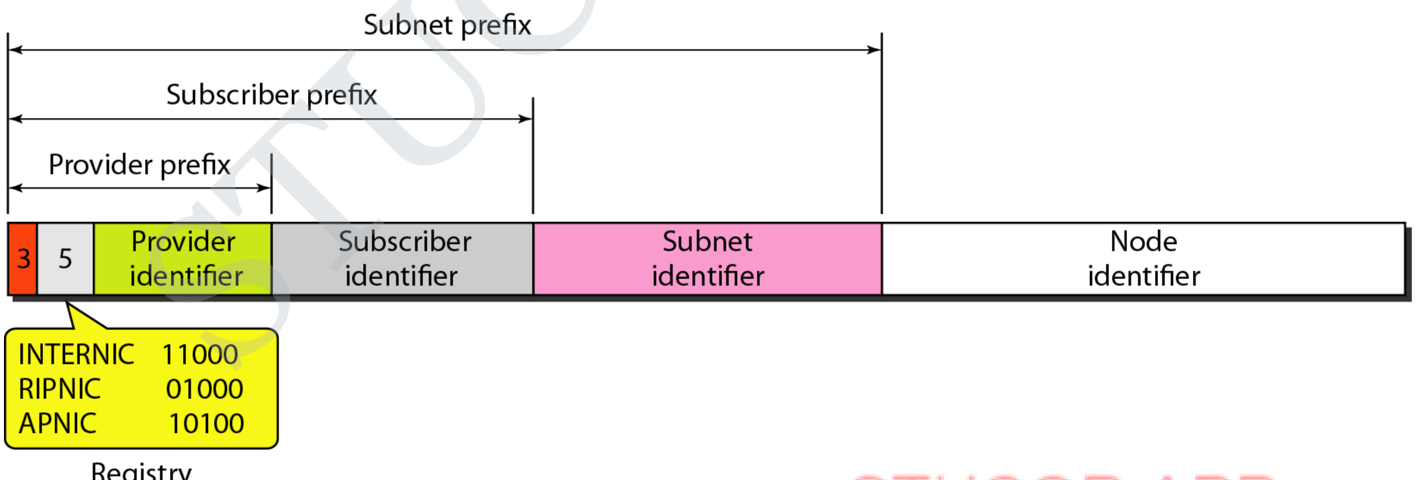
Type Prefix	*Type*	*Fraction*
0000 0000	Reserved	1/256
0000 0001	Unassigned	1/256
0000 001	ISO network addresses	1/128
0000 010	IPX (Novell) network addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Reserved	1/16
001	Reserved	1/8
010	**Provider-based unicast addresses**	**1/8**

Type prefixes for IPv6 addresses

Type Prefix	*Type*	*Fraction*
011	Unassigned	1/8
100	Geographic-based unicast addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

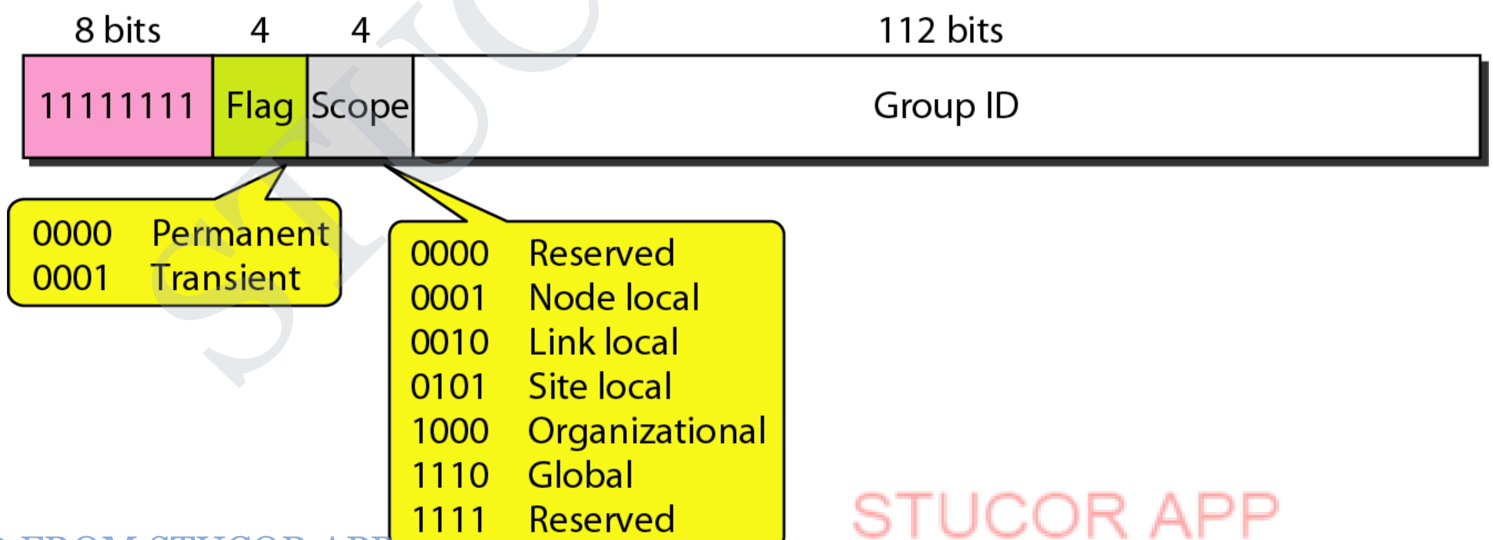
Unicast

- For a single computer
- Two types of unicast addresses
  - Geographically based
  - Provider-based
- Fields
  - Type ID (3-bit), Registry ID (5-bit), Provider ID (16-bit), Subscriber ID (24-bit), Subnet ID (32-bit), Node ID (48-bit)

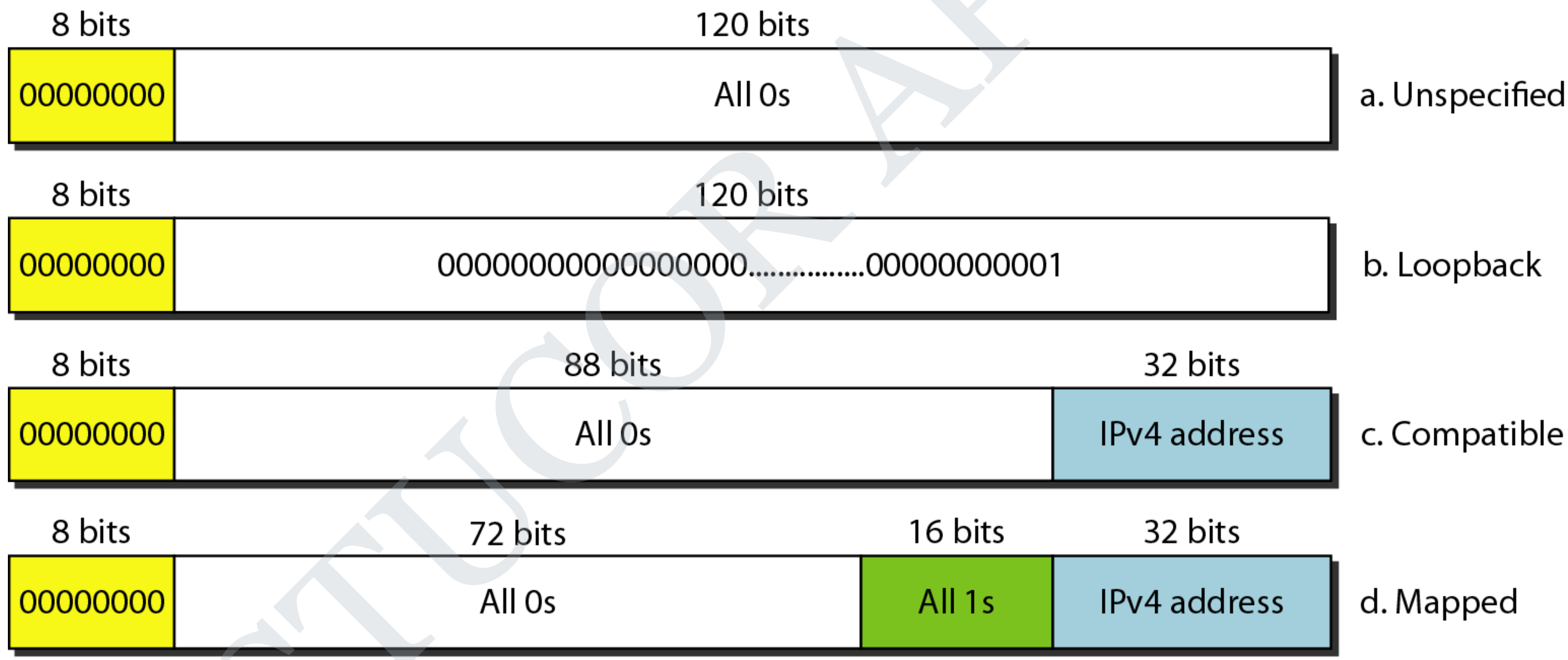


Multicast address in IPv6

- For a group of hosts
- To deliver packets to each member



Reserved addresses in IPv6



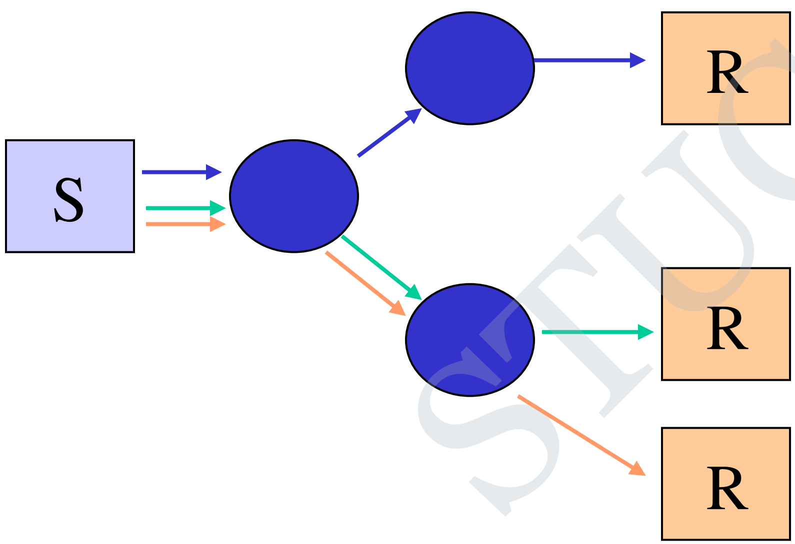
Multicast

Outline

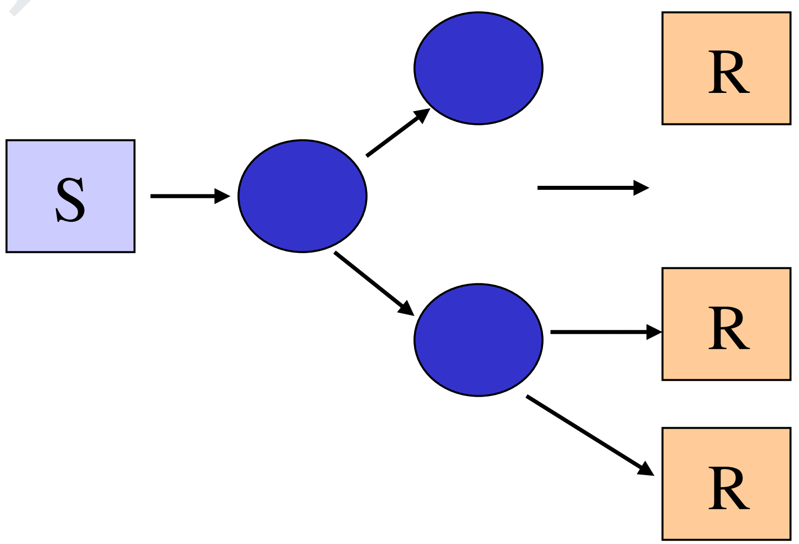
- Multicast Introduction and Motivation
- RIP-based and Protocol Independent Multicast Routing

One to many communication

- Application level one to many communication
- multiple unicasts



- IP multicast



Why Multicast

- When sending same data to multiple receivers
  - better bandwidth utilization
  - less host/router processing
  - quicker participation
- Application
  - Video/Audio broadcast (One sender)
  - Video conferencing (Many senders)
  - Real time news distribution
  - Interactive gaming

IP multicast service model

- Invented by Steve Deering (PhD. 1991)
  - It's a different way of routing datagrams
- RFC1112 : Host Extensions for IP Multicasting - 1989
- Senders transmit IP datagrams to a "host group"
- "Host group" identified by a class D IP address
- Members of host group could be present anywhere in the Internet
- Members join and leave the group and indicate this to the routers
- Senders and receivers are distinct: i.e., a sender need not be a member
- Routers listen to all multicast addresses and use multicast routing protocols to manage groups

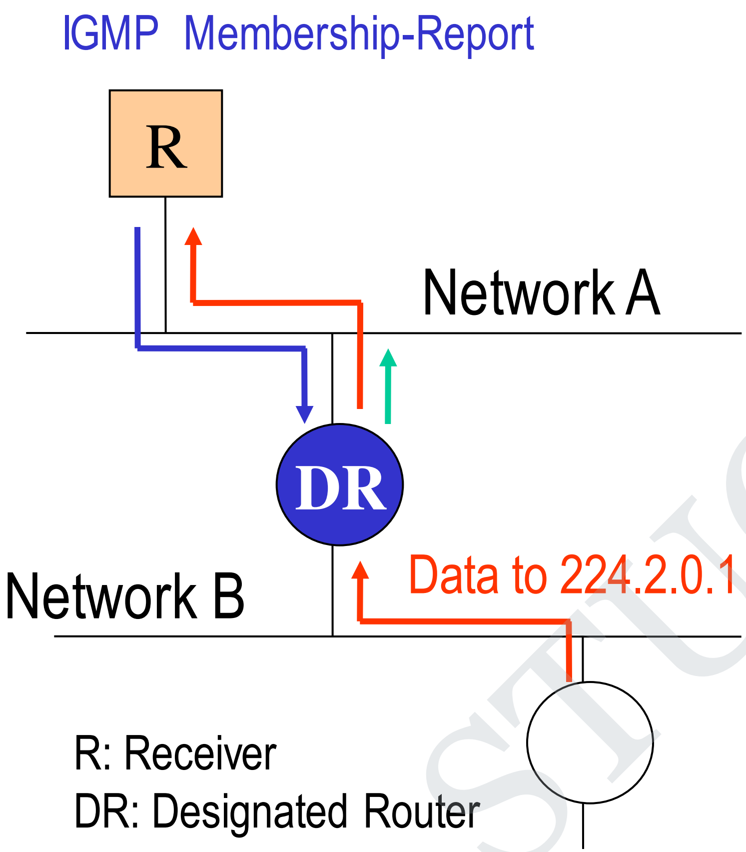
IP multicast group address

- Things are a little tricky in multicast since receivers can be *anywhere*
- Class D address space
  - high-order three 3bits are set
  - 224.0.0.0 ~ 239.255.255.255
- Allocation is essentially random – any class D can be used
  - Nothing prevents an app from sending to any multicast address
  - Customers end hosts and ISPs are the ones who suffer
- Some well-known address have been designated
  - RFC1700
  - 224.0.0.0 ~ 224.0.0.25
- Standard are evolving

Getting Packets to End Hosts

- We haven't treated general methods for this yet but the problem is having both a unicast and multicast IP
- Packets from remote sources will only be forwarded by IP routers onto a local network only if they know there is at least one recipient for that group on that network
- Internet Group Management Protocol (IGMP, RFC2236)
  - Used by end hosts to signal that they want to join a specific multicast group
  - Used by *routers* to discover what groups have have interested member hosts on each network to which they are attached.
  - Implemented directly over IP

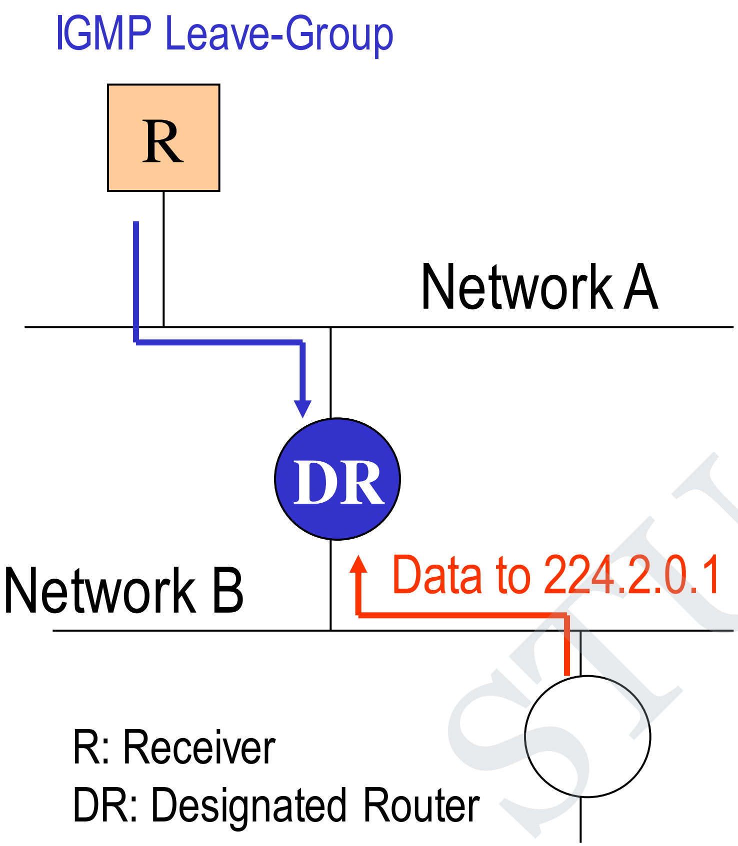
IGMP – Joining a group



Example : R joins to Group 224.2.0.1

- R sends **IGMP Membership-Report to 224.2.0.1**
- DR receives it. DR will start forwarding **packets for 224.2.0.1** to Network A
- DR periodically sends **IGMP Membership-Query to 224.0.0.1** (ALL-SYSTEMS.MCAST.NET)
- R answers **IGMP Membership-Report to 224.2.0.1**

IGMP – Leaving a group



Example : R leaves from a Group 224.2.0.1

- R sends **IGMP Leave-Group to 224.0.0.2** (ALL-ROUTERS.MCAST.NET)
- DR receives it.
- DR stops forwarding **packets for 224.2.0.1** to Network A if no more 224.2.0.1 group members on Network A.

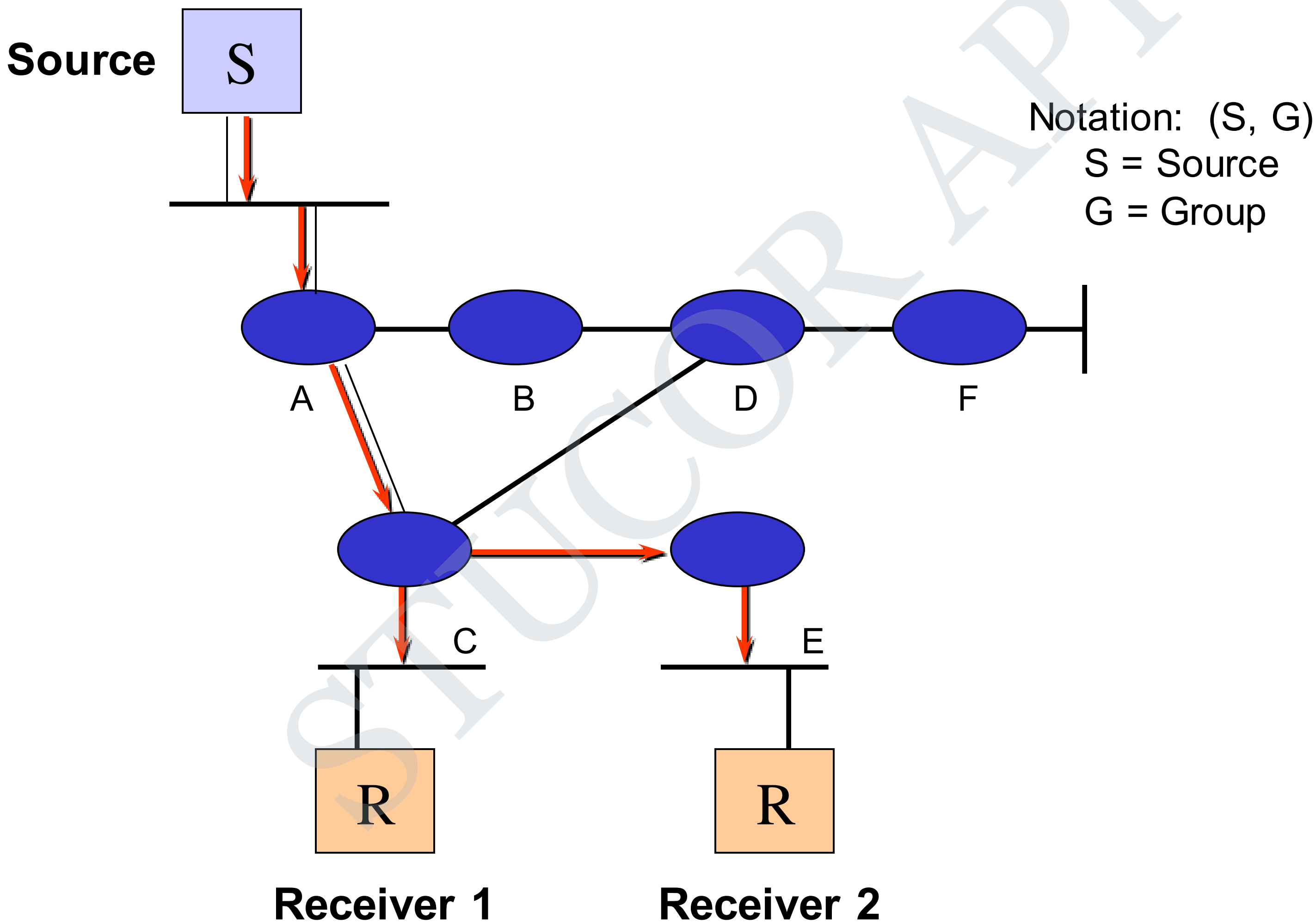
Challenges in the multicast model

- How can a sender restrict who can receive?
  - need authentication, authorization
  - encryption of data
  - key distribution
  - still an active area of research

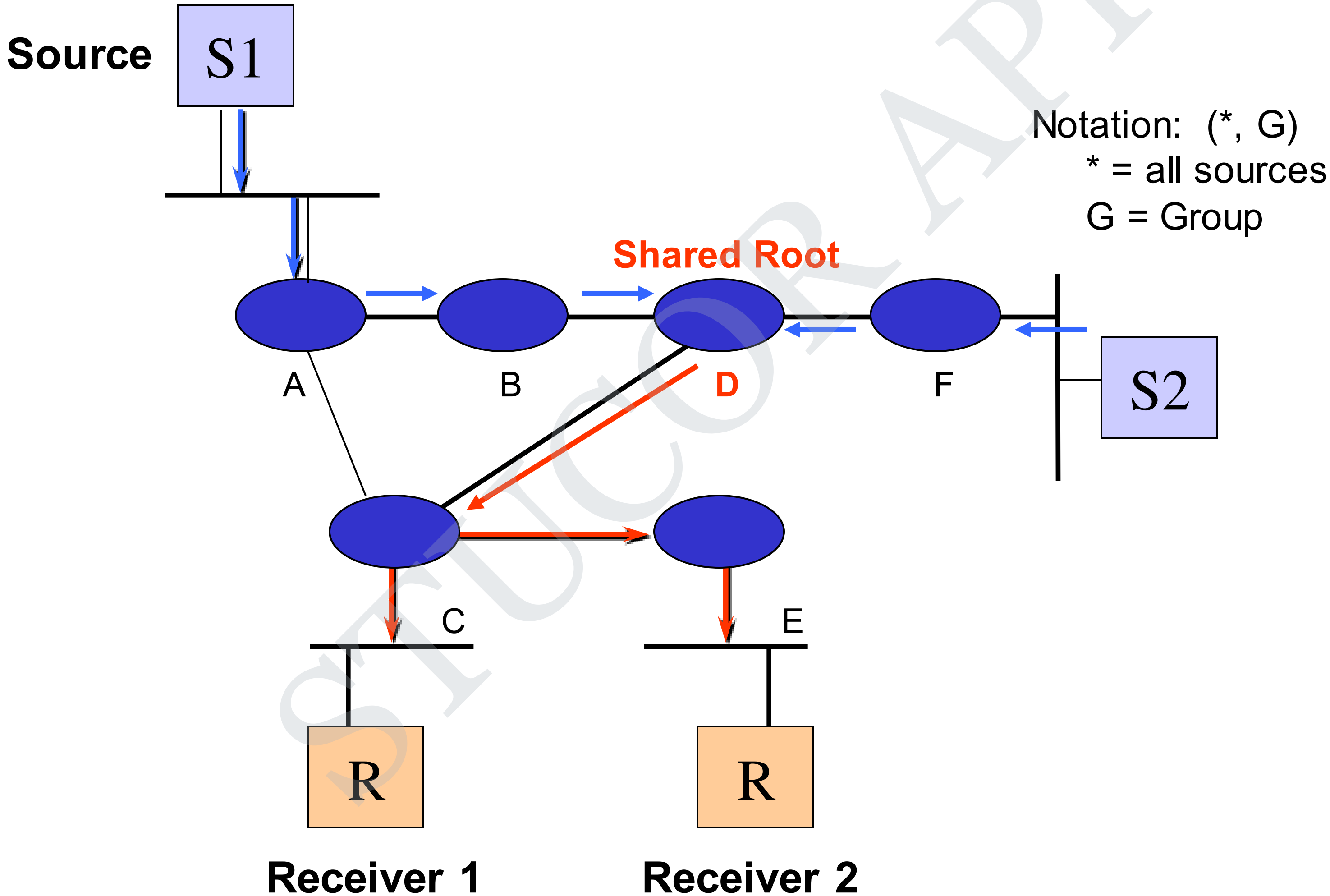
IP multicast routing

- Purpose: share Group information among routers, to implement better routing for data distribution
- Distribution tree structure
  - Source tree vs shared tree
- Data distribution policy
  - Opt in (ACK) type vs opt out (NACK) type
- Routing protocols are used in conjunction with IGMP

Source distribution tree



Shared distribution tree



Source tree characteristics

- Source tree
  - More memory O (G x S) in routers
  - optimal path from source to receiver, minimizes delay
- good for
  - small number of senders, many receivers such as Radio broadcasting application

Shared tree characteristics

- Shared tree
  - Less memory O (G) in routers
  - Sub-optimal path from source to receiver, may introduce extra delay (source to root)
  - May have duplicate data transfer (possible duplication of a path from source to root and a path from root to receivers)
- good for
  - Environments where most of the shared tree is the same as the source tree
  - Many senders with low bandwidth (e.g. shared whiteboard)

Data distribution policy

- Opt out (NACK) type
  - Start with “broadcasting” then prune brunches with no receivers, to create a distribution tree
  - Lots of wasted traffic when there are only a few receivers and they are spread over wide area
- Opt in (ACK) type
  - Forward only to the hosts which explicitly joined to the group
  - Latency of join propagation

Protocol types

- Dense mode protocols
  - assumes dense group membership
  - Source distribution tree and NACK type
  - **DVMRP** (Distance Vector Multicast Routing Protocol)
  - **PIM-DM** (Protocol Independent Multicast, Dense Mode)
  - Example: Company-wide announcement
- Sparse mode protocol
  - assumes sparse group membership
  - Shared distribution tree and ACK type
  - **PIM-SM** (Protocol Independent Multicast, Sparse Mode)
  - Examples: Futurama or a Shuttle Launch

DVMRP

exchange distance vectors

- Each router maintains a 'multicast routing table' by exchanging distance vector information among routers
  - First multicast routing protocol ever deployed in the Internet
    - Similar to RIP
  - Constructs a source tree for each group using reverse path forwarding
    - Tree provides a shortest path between source and each receiver
- There is a "designated forwarder" in each subnet
  - Multiple routers on the same LAN select designated forwarder by lower metric or lower IP address (discover when exchanging metric info.)
- Once tree is created, it is used to forward messages from source to receivers
- If all routers in the network do not support DVMRP then unicast tunnels are used to connect multicast enabled networks

DVMRP

broadcast & prune

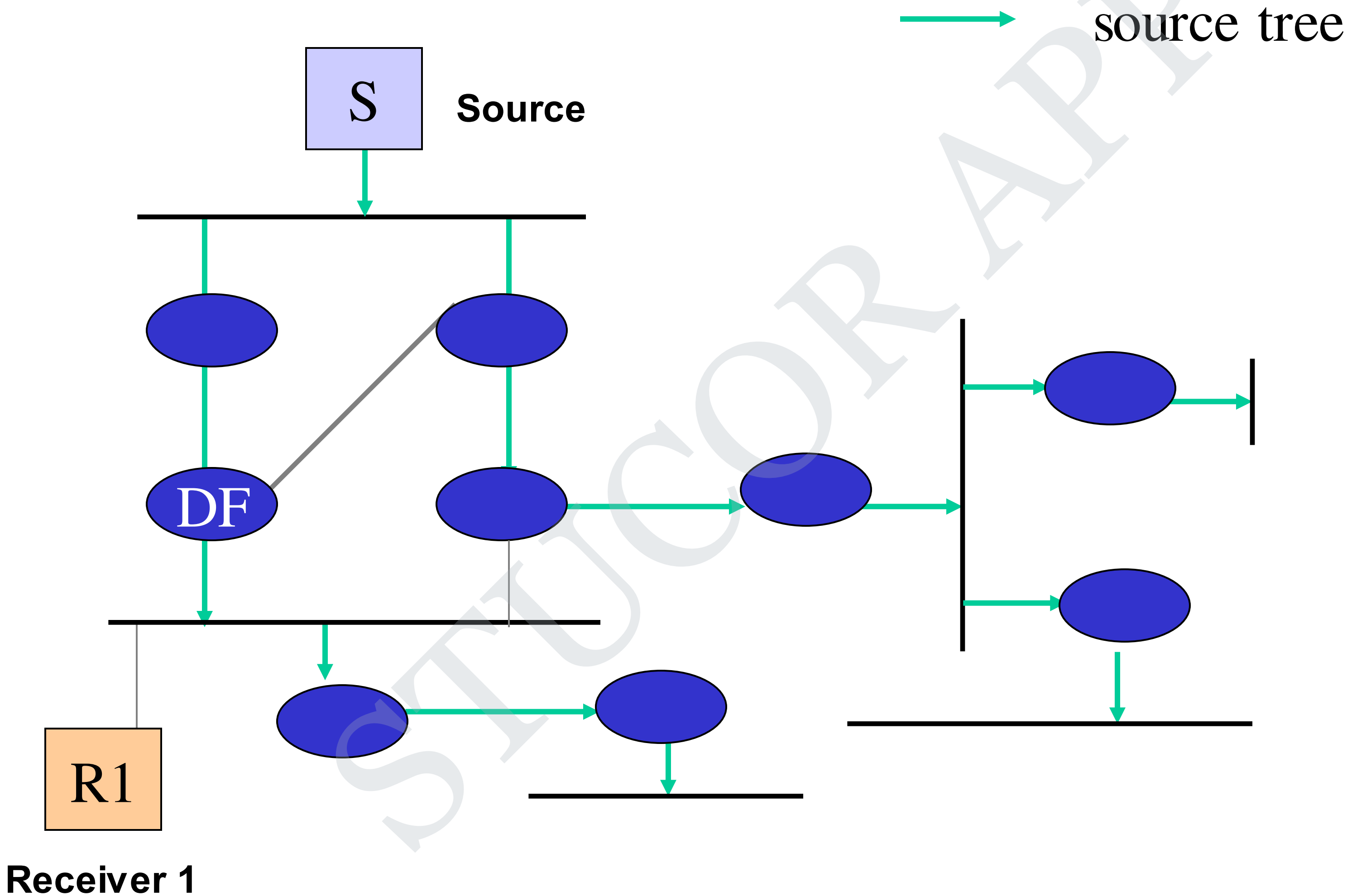
- Flood multicast packets based on RPF (Reverse path forwarding) rule to all routers.
- Leaf routers check and sends prune message to upstream router when no group member is on their network
- Upstream router prune the interface with no dependent downstream router.
- *Graft* message to create a new branch for late participants
- Restart forwarding after prune lifetime (standard : 720 minutes)
- draft-ietf-idmr-dvmrp-v3-09.txt (September 1999)

RPF(reverse path forwarding)

- Simple algorithm developed to avoid duplicate packets on multi-access links
- RPF algorithm takes advantage of the IP routing table to compute a multicast tree for each source.
- RPF check
  1. When a multicast packet is received, note its source (*S*) and interface (*I*)
  2. If *I* belongs to the shortest path from *S*, forward to all interfaces except *I*
  3. If test in step 2 is false, drop the packet
- Packet is never forwarded back out the RPF interface!

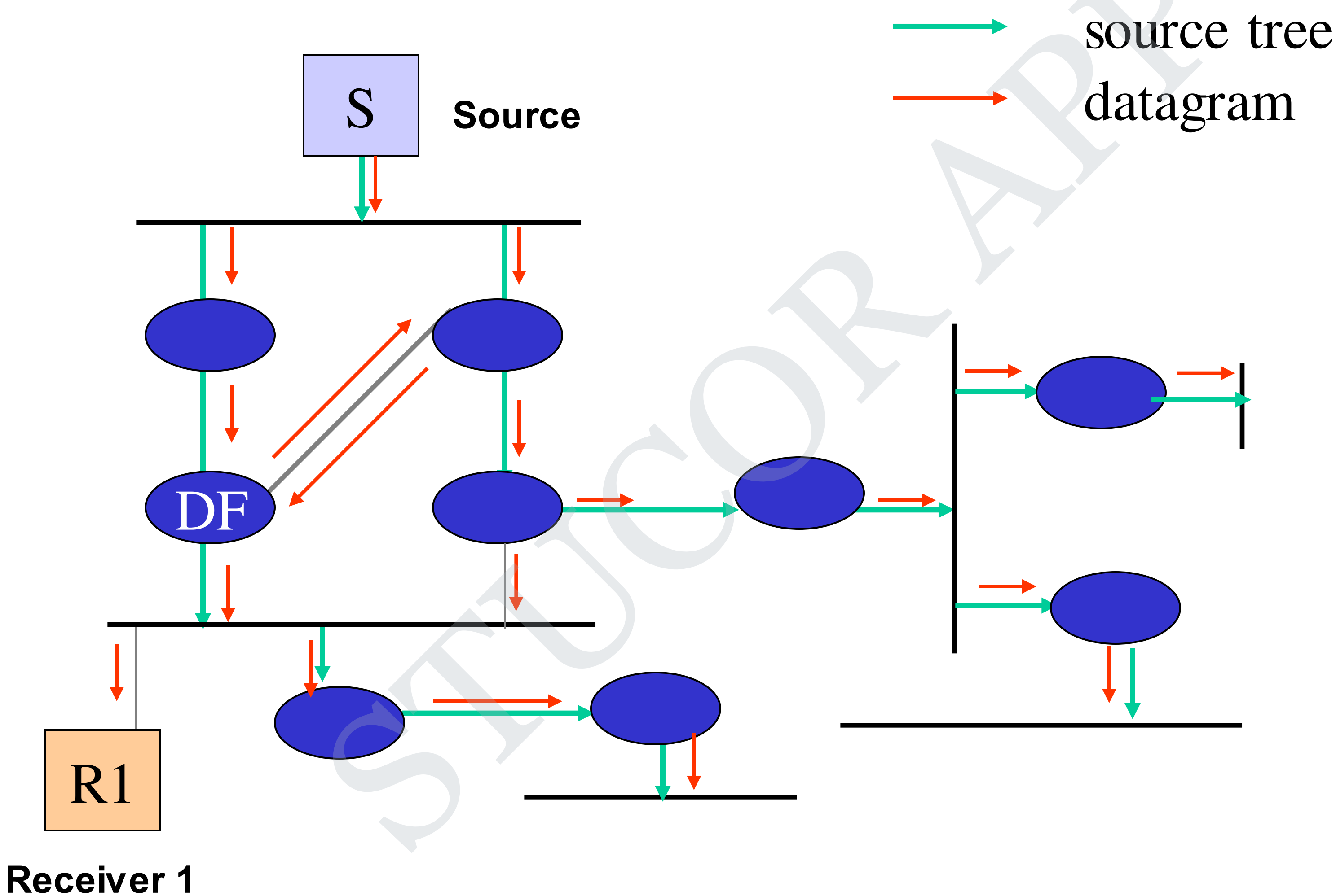
DVMRP (1)

form a source tree by exchanging metric



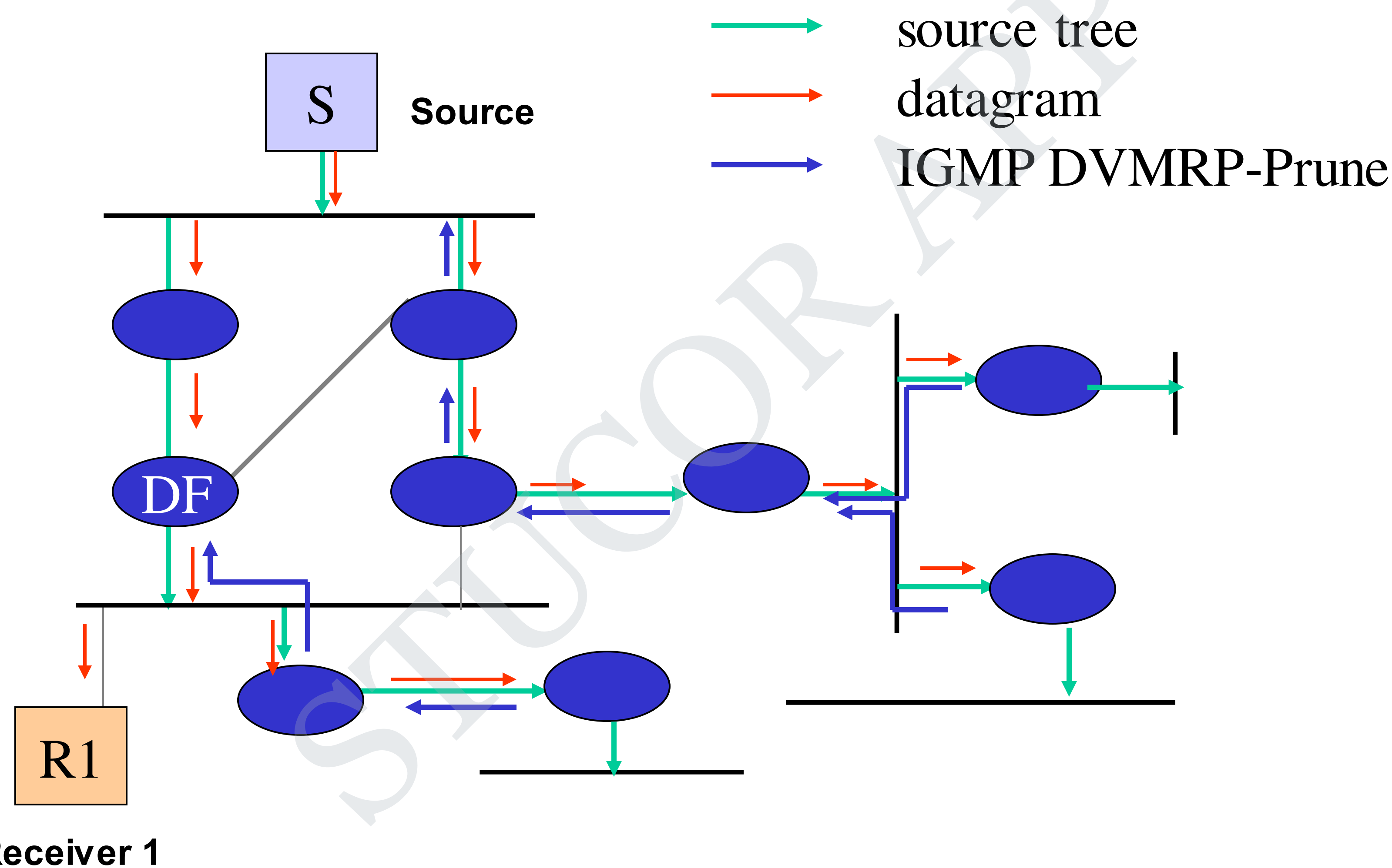
DVMRP (2)

broadcast



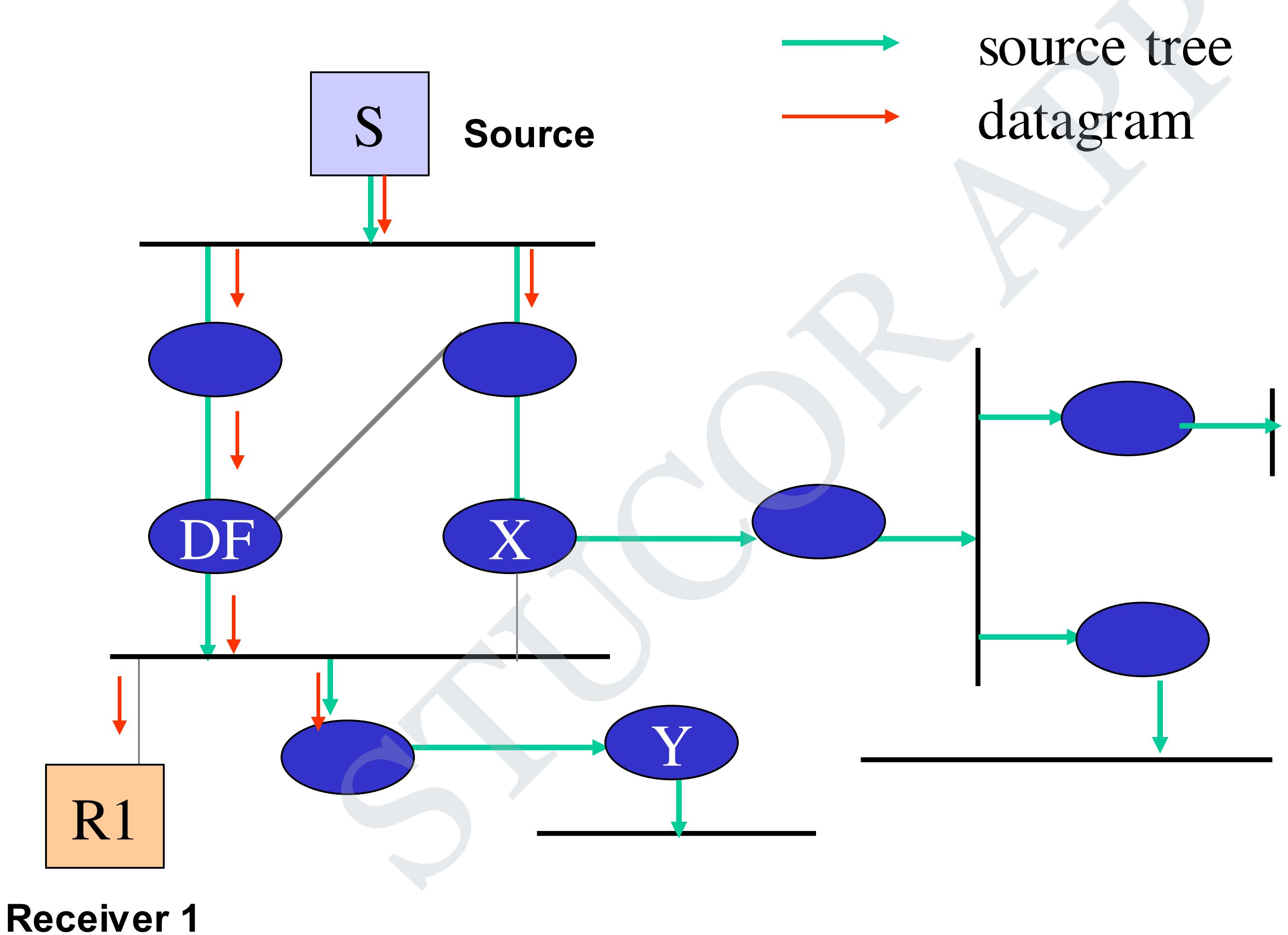
DVMRP (3)

prune



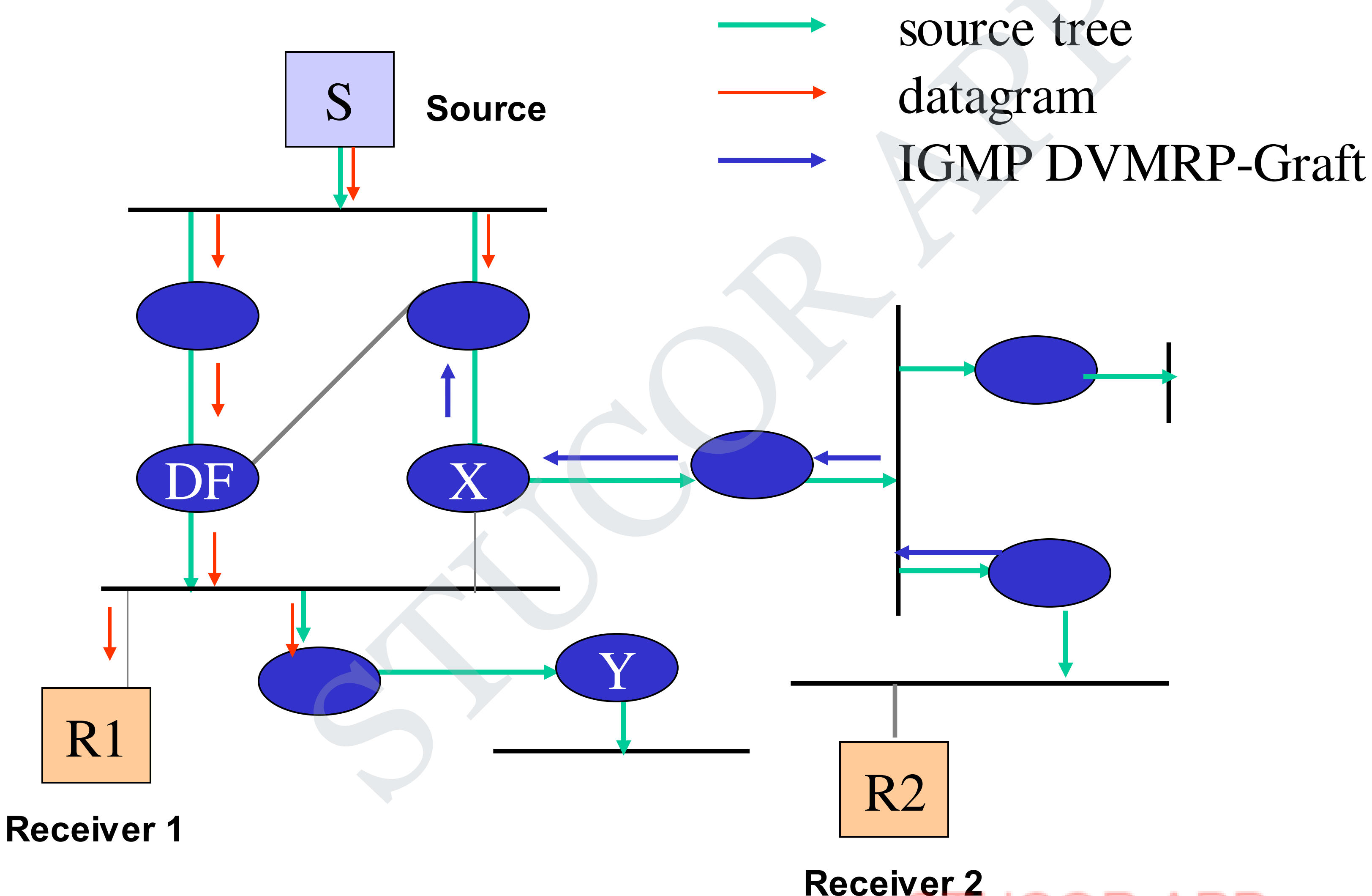
DVMRP (4)

X and Y pruned



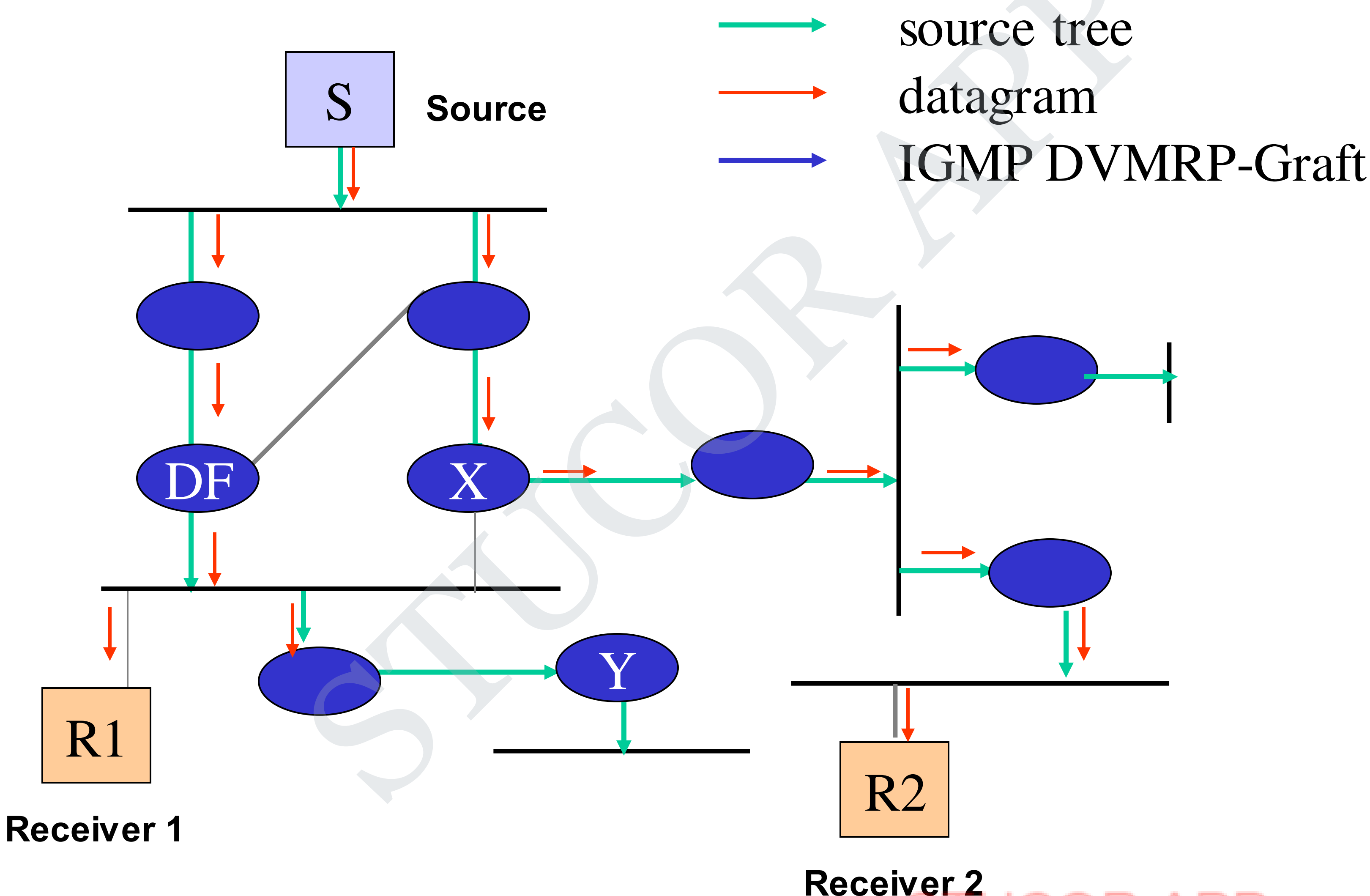
DVMRP (4)

New member



DVMRP (4)

New branch



Protocol Independent Multicast

- PIM : Protocol Independent Multicast
  - Independent of particular unicast routing protocol
    - Just assumes one exists
  - Pros: simple, less overhead
    - Does not require computation of specific routing tables
  - Cons: may cause more broadcast-and-prunes (in dense mode)
  - Most popular multicast routing protocol today
- Main difference with DVMRP – independence from underlying unicast routing mechanism
- PIM supports both *dense* (DM) and *sparse* (SM) mode operation
  - You can locally use either or both modes

PIM DM overview(1)

- Assumes that you have lots of folks who want to be part of a group
- Based on broadcast and prune
  - Ideal for dense group
- Source tree created on demand based on RPF rule
- If the source goes inactive, the tree is torn down
- Easy “plug-and-play” configuration
- Branches that don’t want data are pruned

PIM DM overview(2)

- *Grafts* used to join existing source tree
- *Asserts* used to determine the forwarder for multi-access LAN
- Non-RPF point-2-point links are pruned as a consequence of initial flooding

PIM DM Forwarding

- PIM DM interfaces are placed on an "downstream" list for a multicast group if:
  - PIM neighbor is heard on interface
  - Host on this interface has just joined the group
  - Interface has been manually configured to join group
- Packets are flooded out all interfaces in "downstream" list
  - If a PIM neighbor is present, DM assumes EVERYONE wants to receive the group so it gets flooded to that link

PIM Assert Mechanism

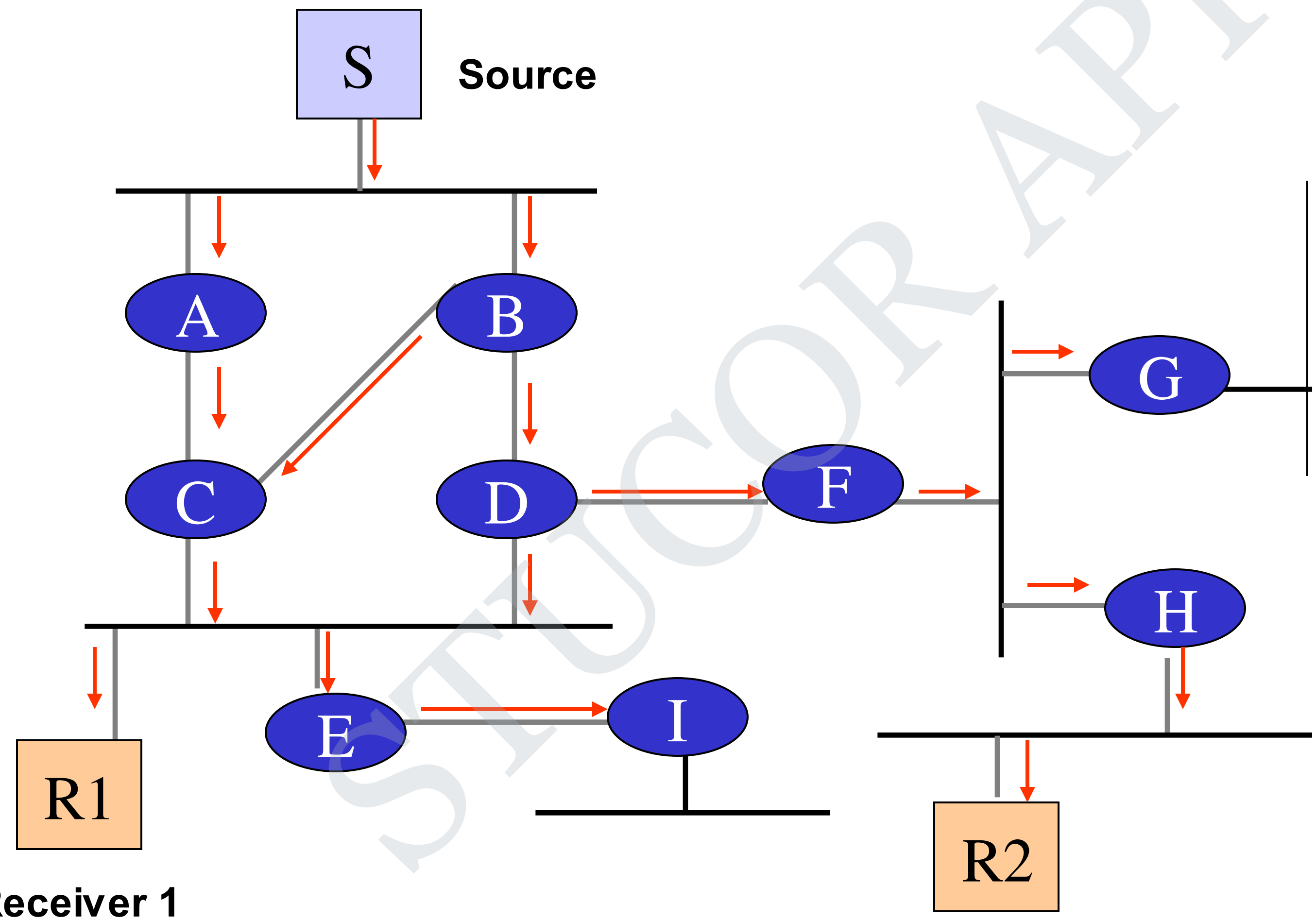
- Routers receive packet on an interface in their “downstream” list
  - Only one router should continue sending to avoid duplicate packets.
- Routers sends “PIM assert” messages
  - Compare distance and metric values
  - Router with best route to source wins
  - If metric & distance equal, highest IP addr wins
  - Losing router stops sending (prunes interface)

PIM DM State Maintenace

- State is maintained by the “flood and prune” behavior of Dense Mode.
  - Received Multicast packets reset(S,G) entry “expiration” timers.
  - When (S,G) entry “expiration” timers count down to zero, the entry is deleted.
- Interface prune state times out causing periodic reflooding and pruning
  - could be as little as 210 seconds

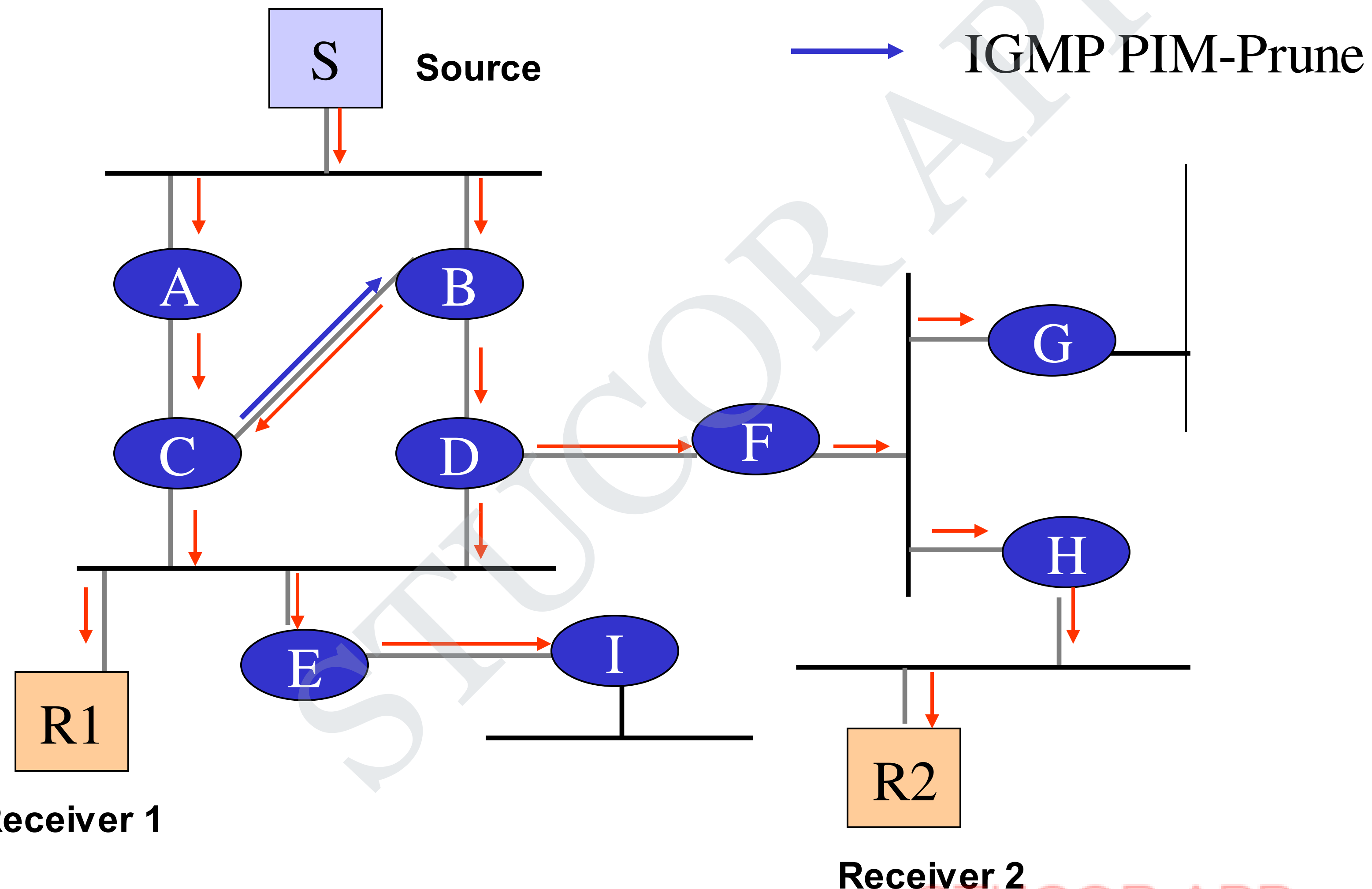
PIM-DM(1)

Initial flood of data



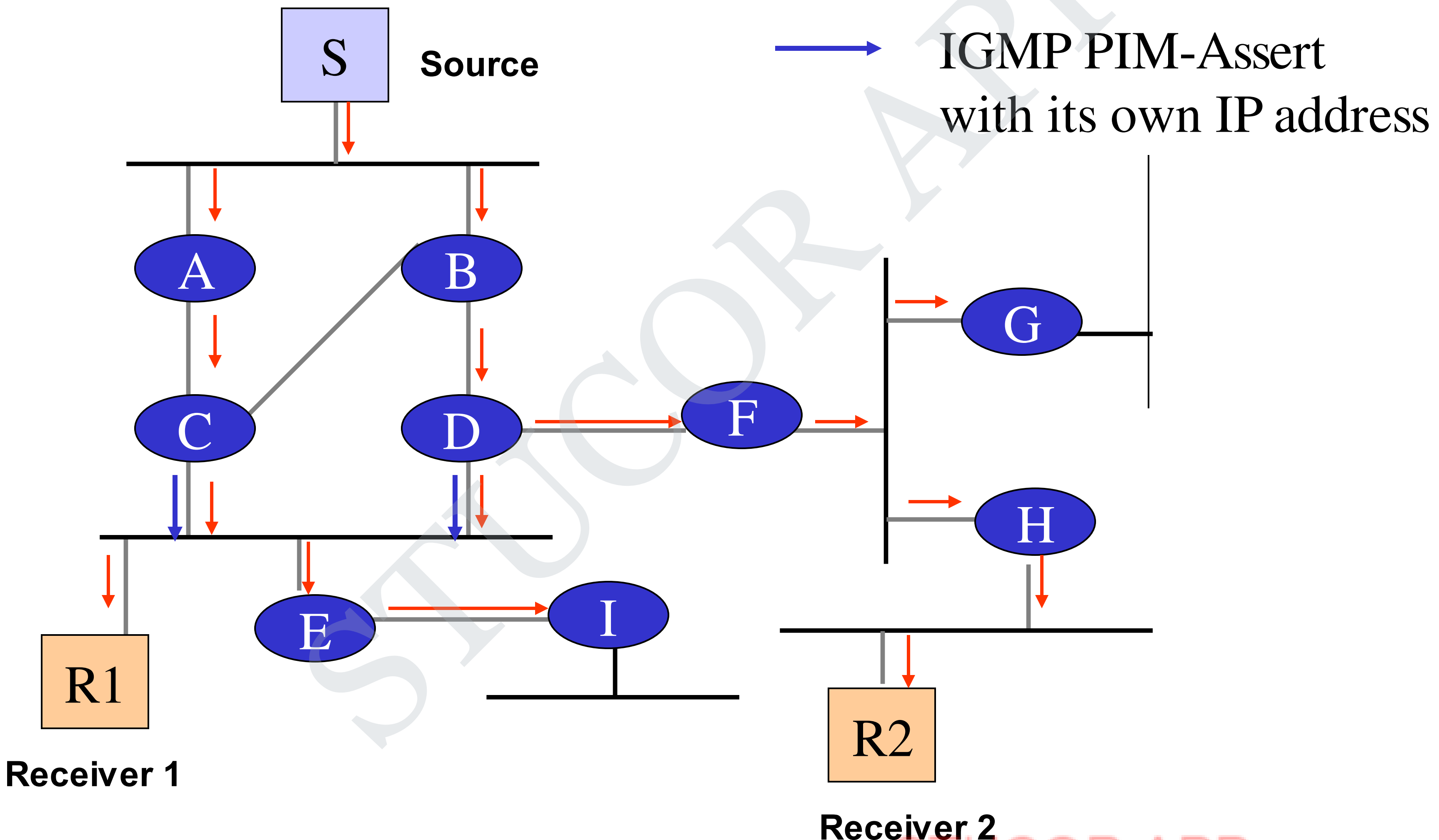
PIM-DM(2)

prune non-RPF p2p link



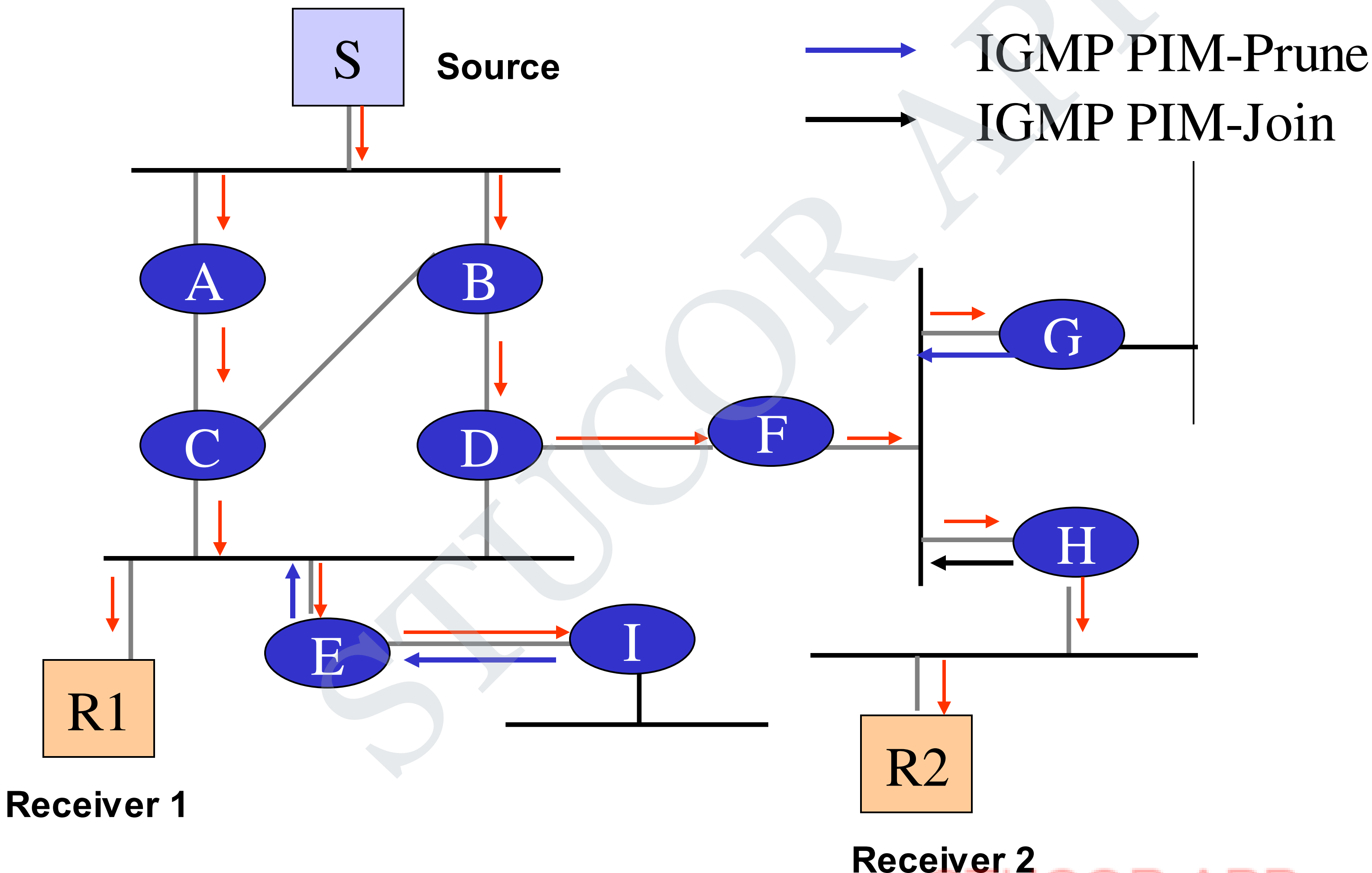
PIM-DM(3)

C and D Assert to Determine Forwarder for the LAN, C Wins



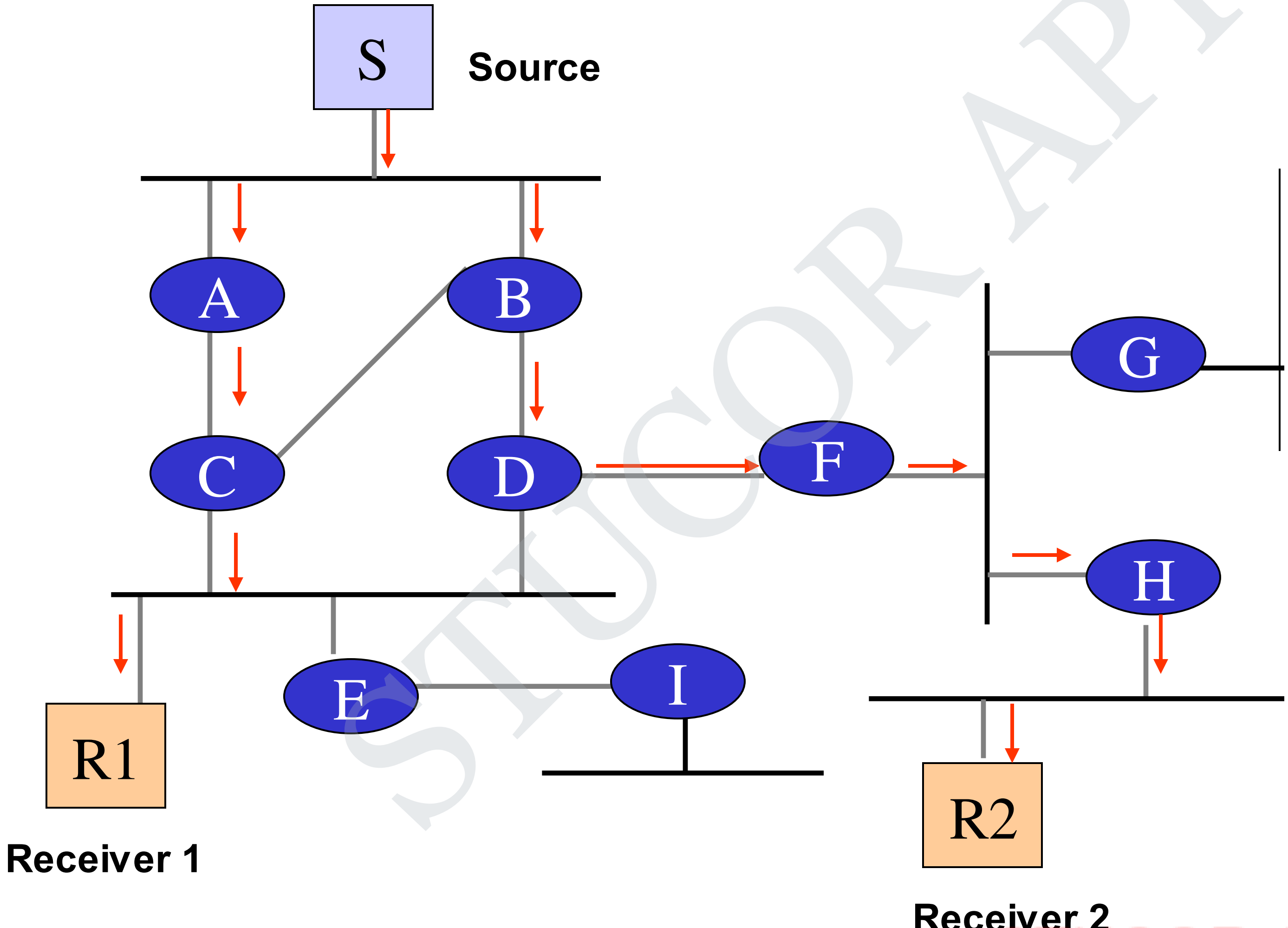
PIM-DM(4)

I, E, G send Prune
H send Join to override G's Prune



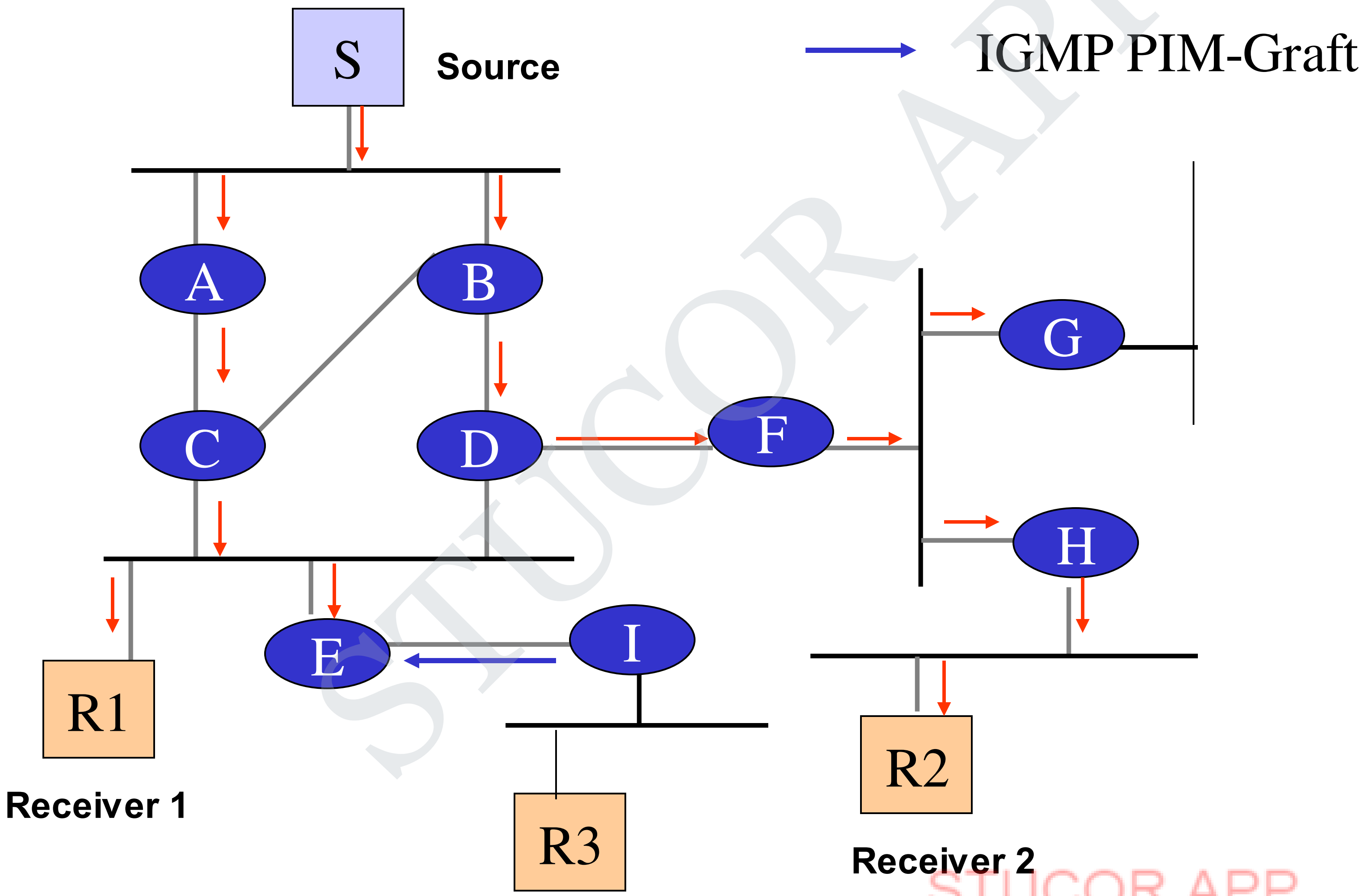
PIM-DM(5)

I Gets Pruned
E's Prune is Ignored (since R1 is a receiver)
G's Prune is Overridden (due to new receiver R2)



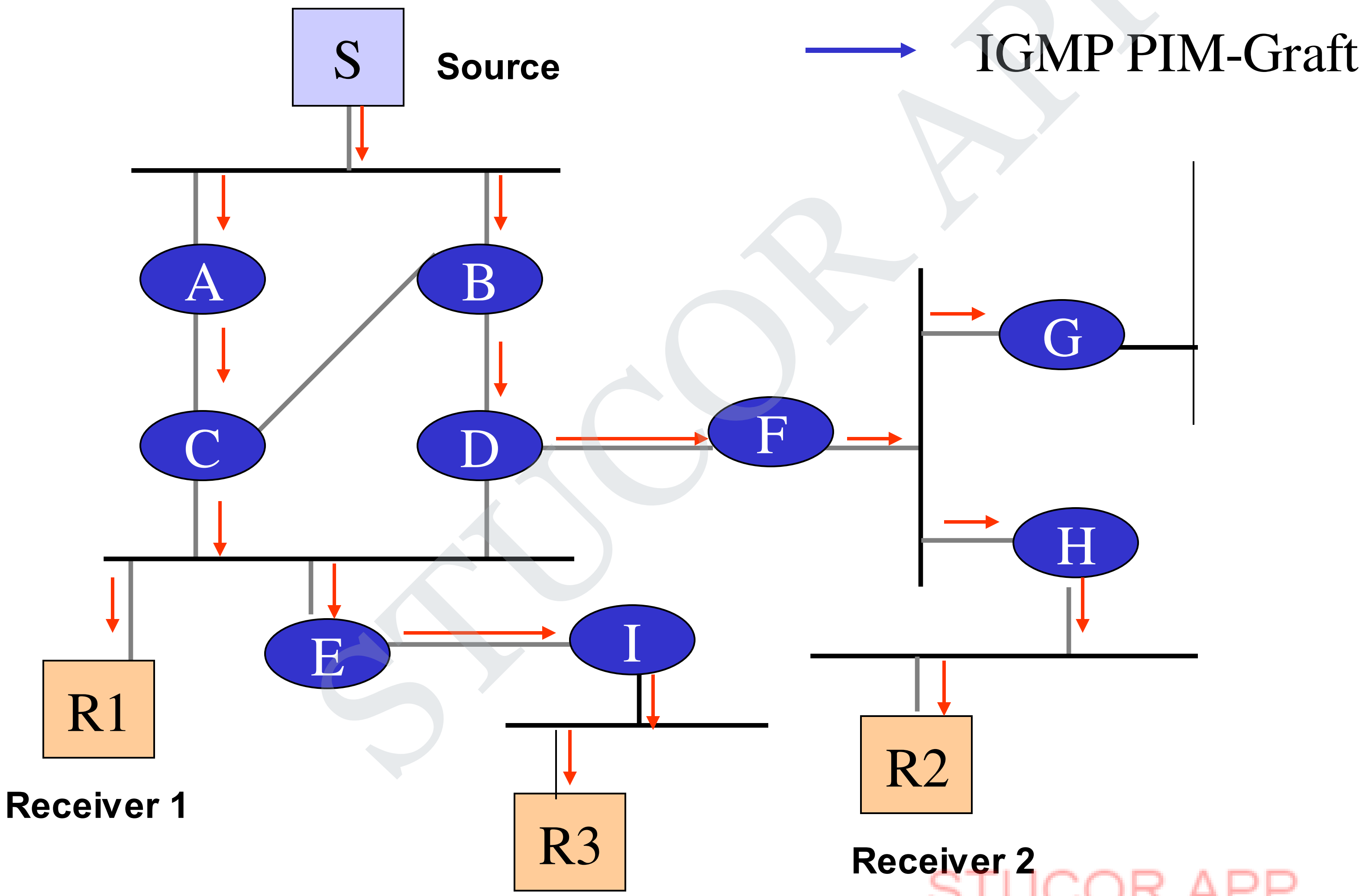
PIM-DM(6)

New Receiver, I send Graft



PIM-DM(6)

new branch



CS8591 – COMPUTER NETWORKS

UNIT –IV

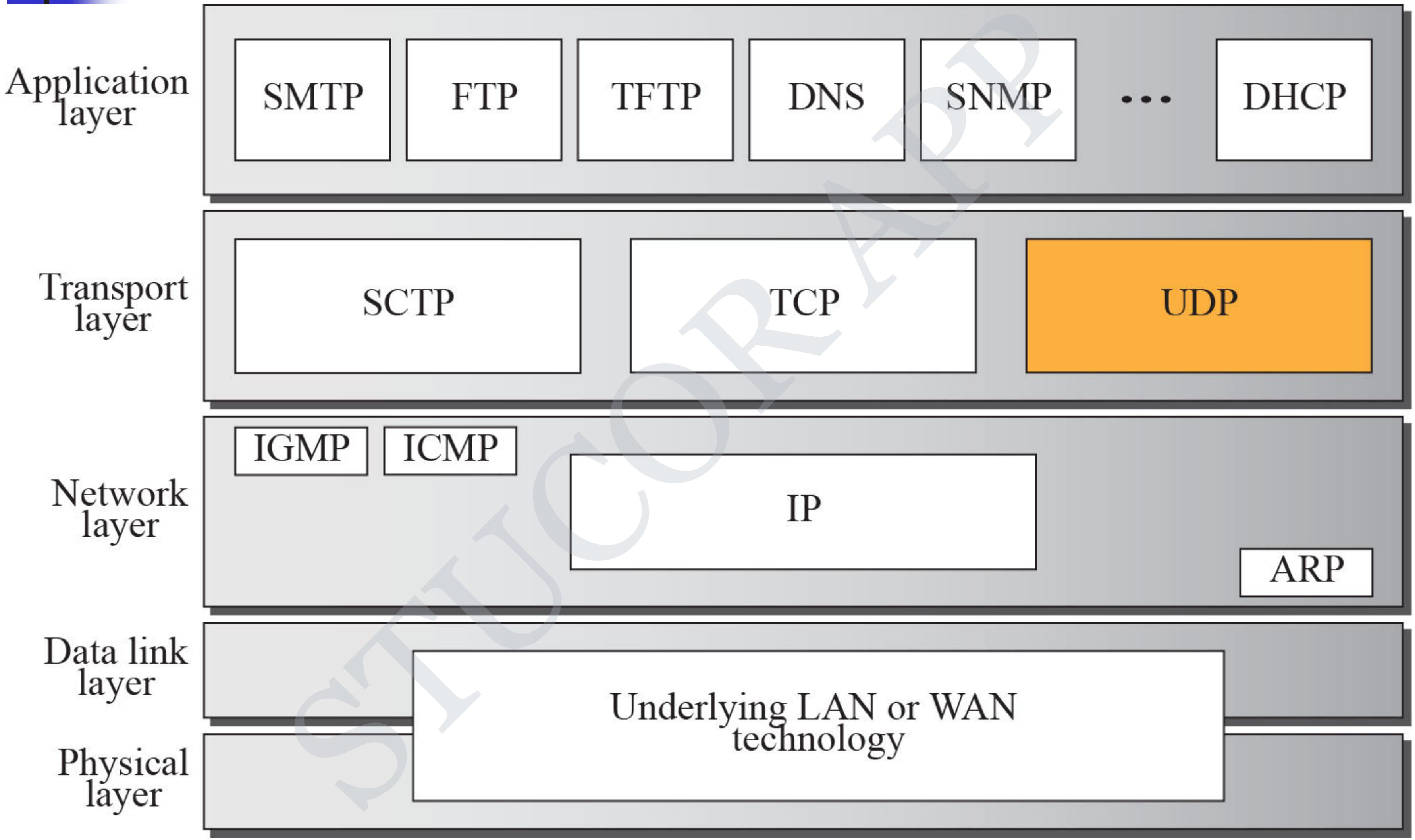
Dr.R.SASIKUMAR
Professor/CSE
R.M.D.Engineering College

TRANSPORT LAYER

UDP

Relationship of the User Datagram Protocol (UDP) to the other protocols and layers of the TCP/IP protocol suite: UDP is located between the application layer and the IP layer, and serves as the intermediary between the application programs and the network operations.

Position of UDP in the TCP/IP protocol suite

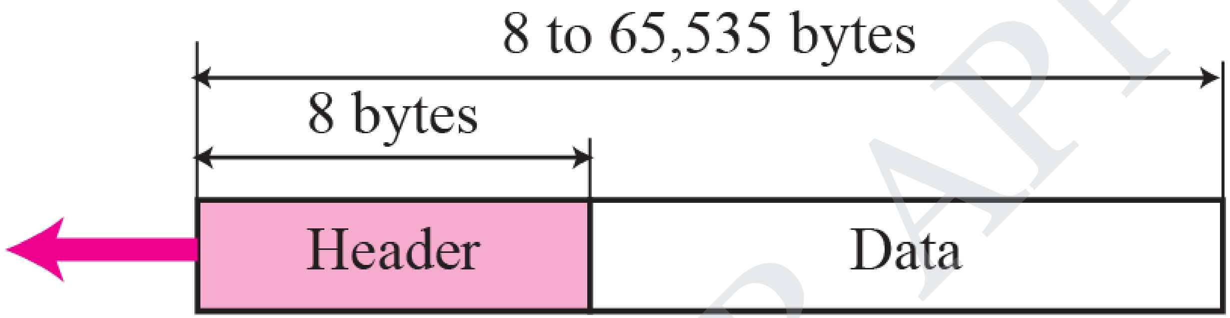


USER DATAGRAM

UDP packets, called user datagrams, have a fixed-size header of 8 bytes. Figure 14.2 shows the format of a user datagram.

DOWNLOADED FROM STUCOR APP

User datagram format



a. UDP user datagram

0 16 31

Source port number	Destination port number
Total length	Checksum

b. Header format

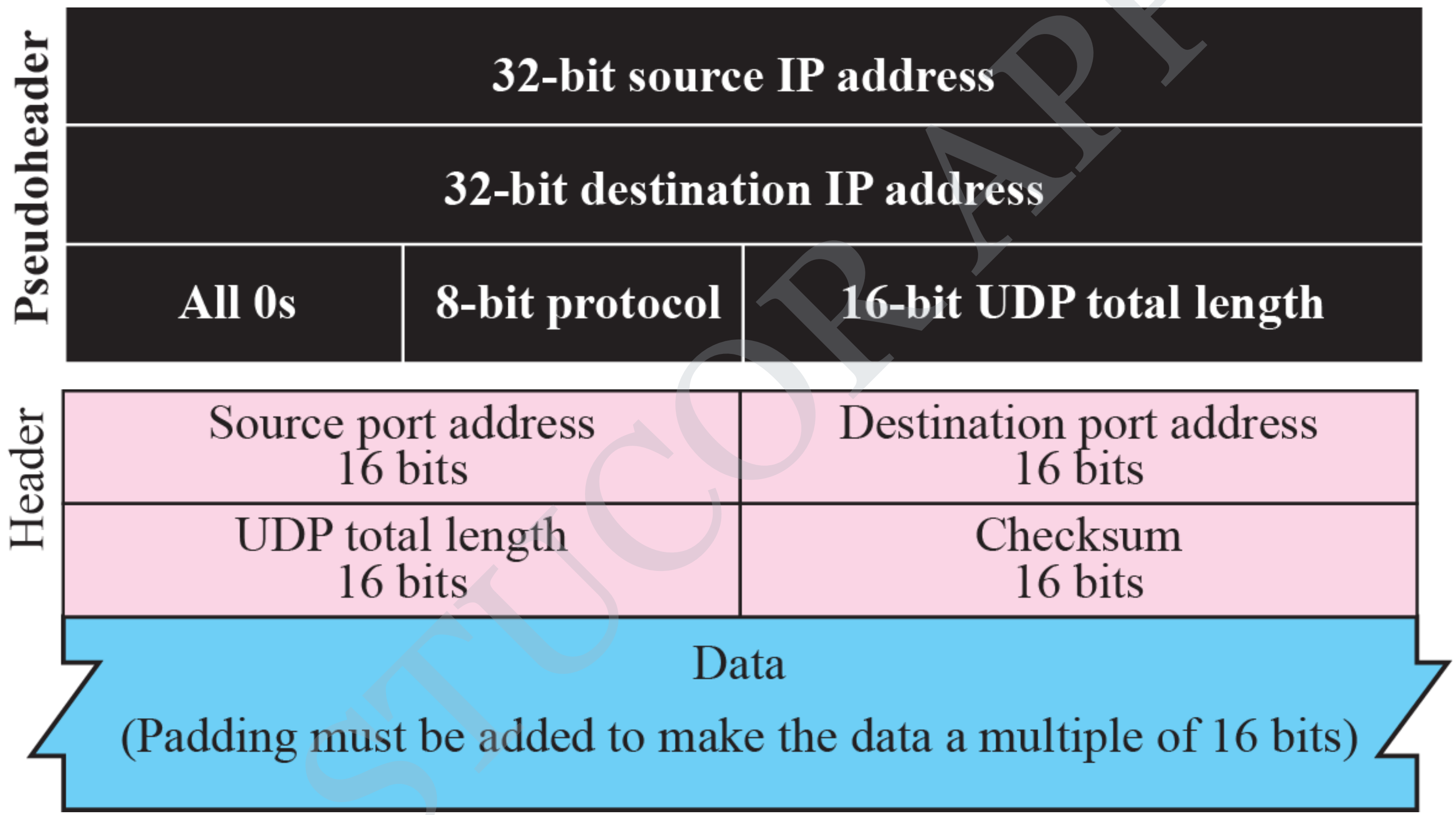
UDP Services

We discussed the general services provided by a transport layer protocol. In this section, we discuss what portions of those general services are provided by UDP.

Table 14.1 *Well-known Ports used with UDP*

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Domain	Domain Name Service (DNS)
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

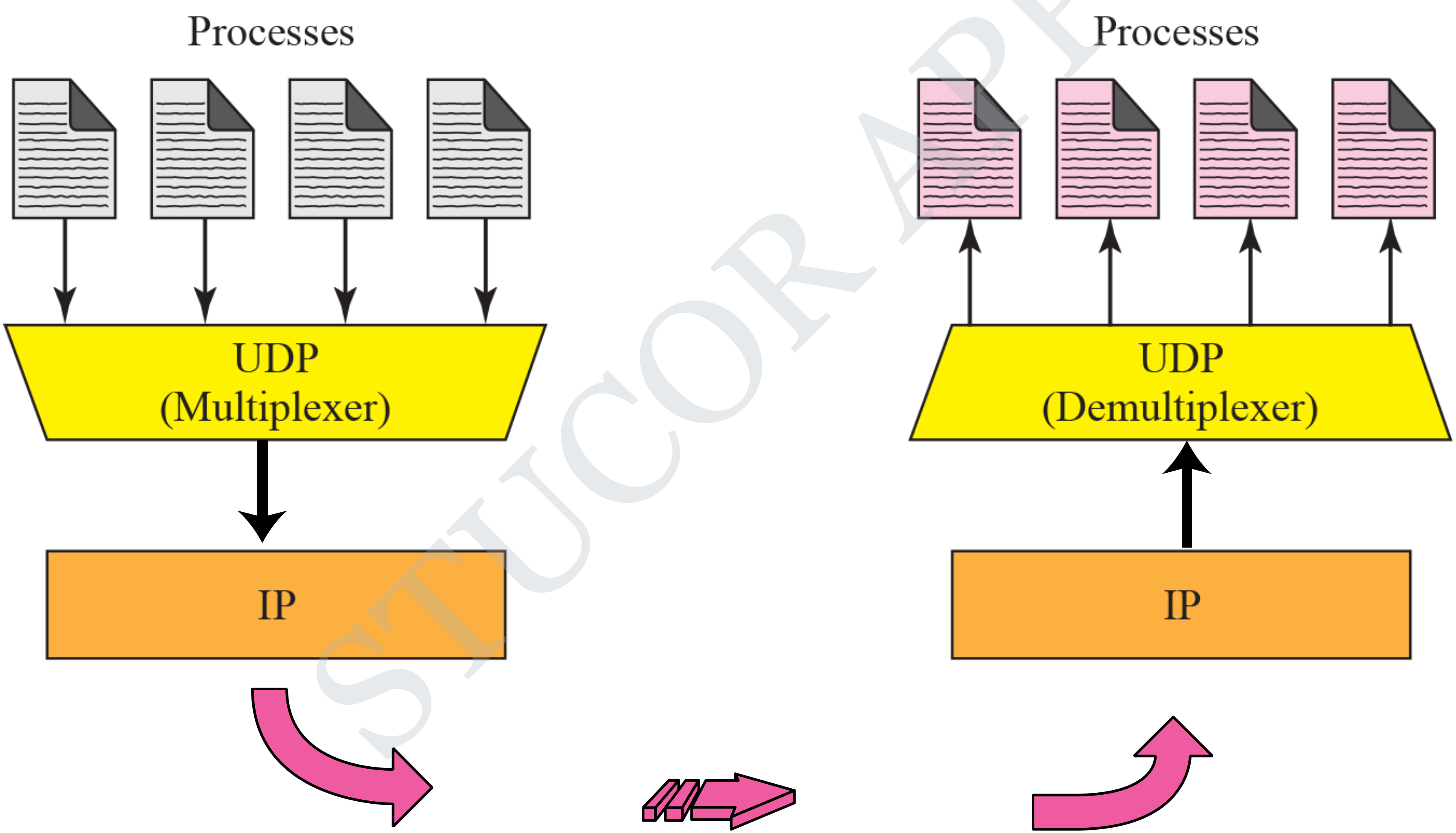
Pseudoheader for checksum calculation



UDP APPLICATION

Although UDP meets almost none of the criteria we mentioned in Chapter 13 for a reliable transport-layer protocol, UDP is preferable for some applications. The reason is that some services may have some side effects that are either unacceptable or not preferable. An application designer needs sometimes to compromise to get the optimum.

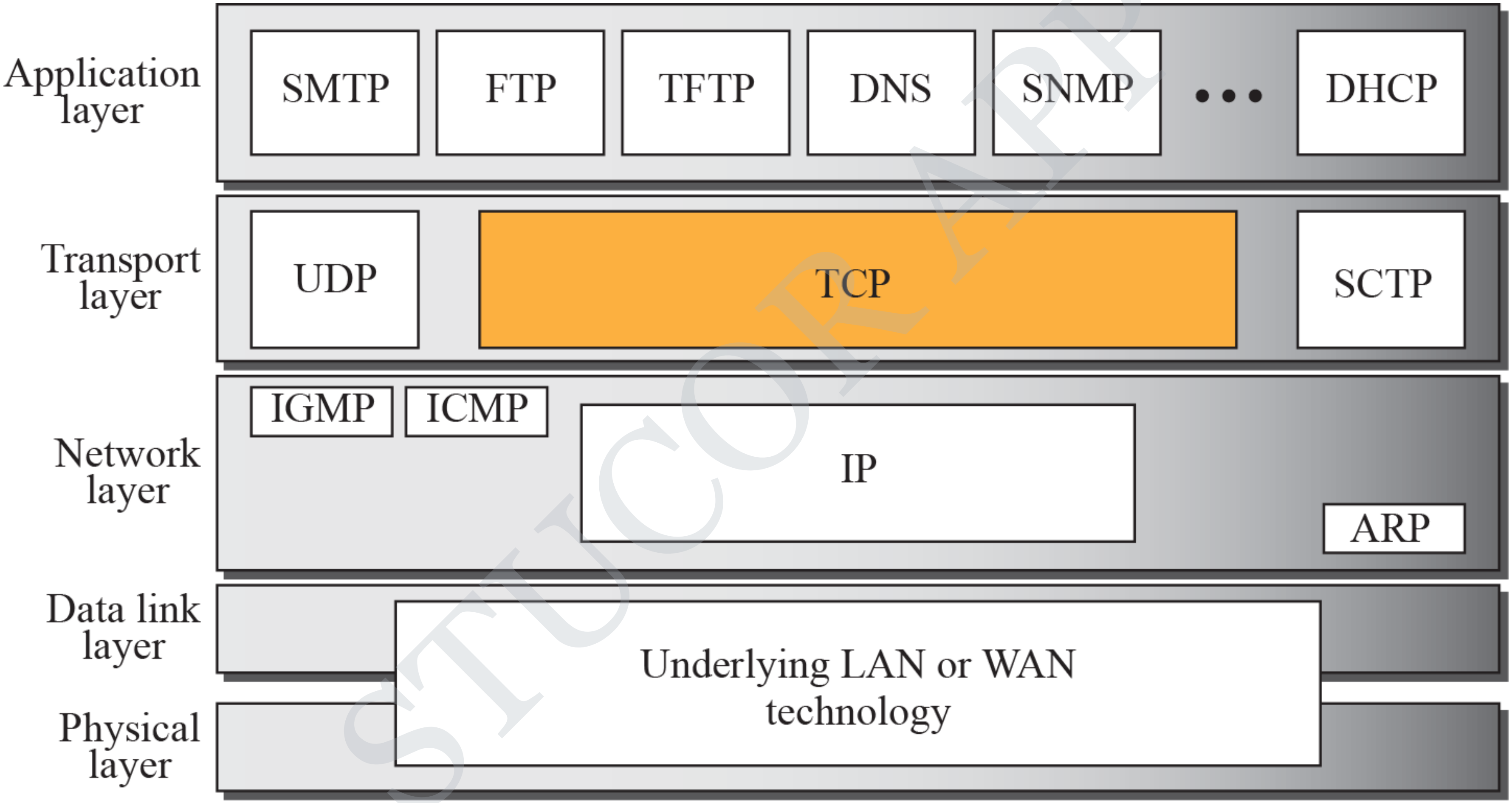
Multiplexing and demultiplexing



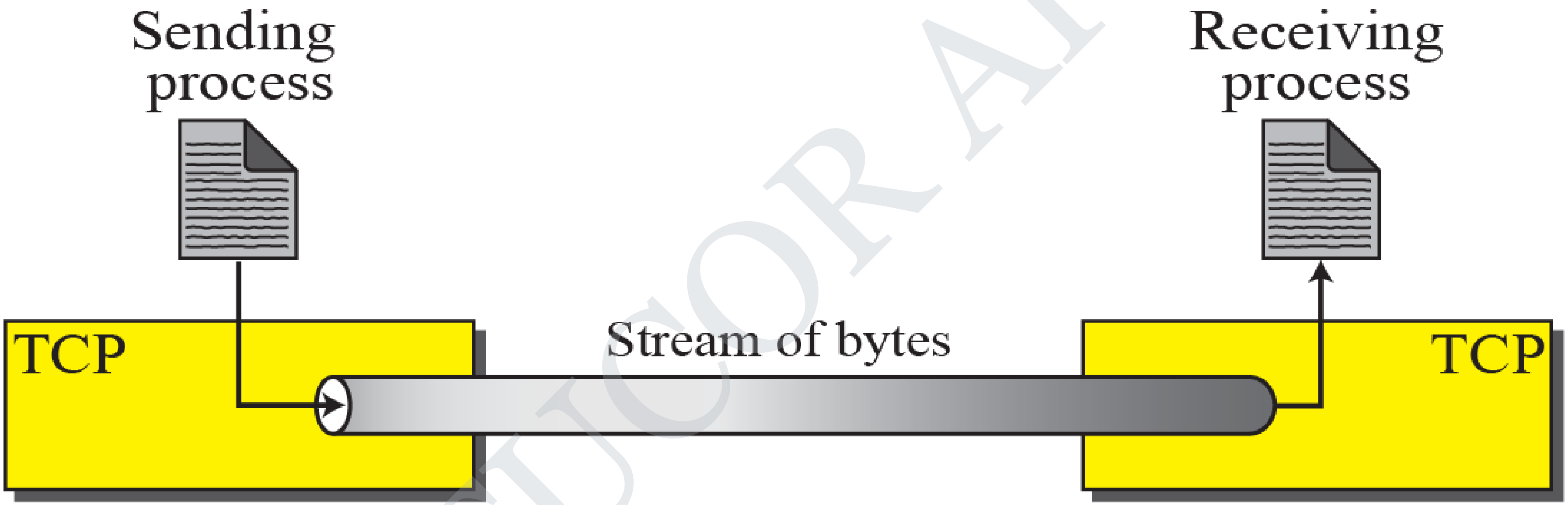
TCP SERVICES

Relationship of TCP to the other protocols in the TCP/IP protocol suite. TCP lies between the application layer and the network layer, and serves as the intermediary between the application programs and the network operations.

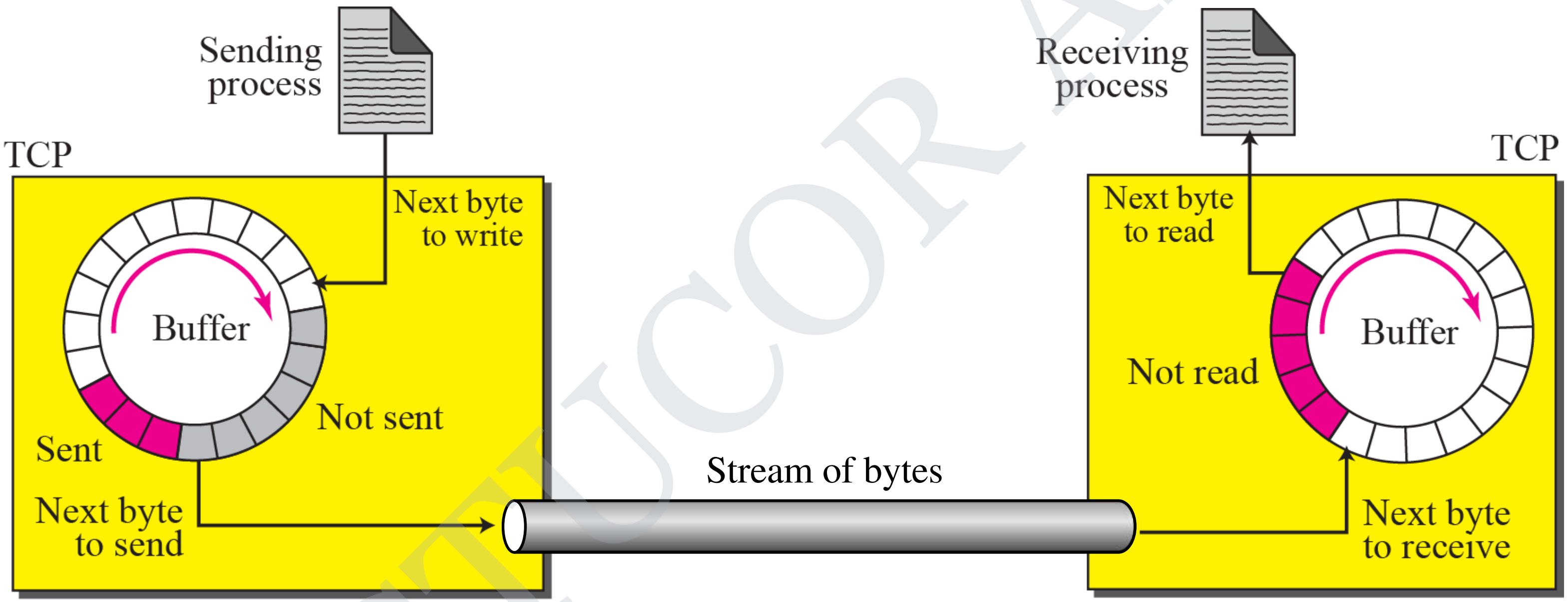
TCP/IP protocol suite



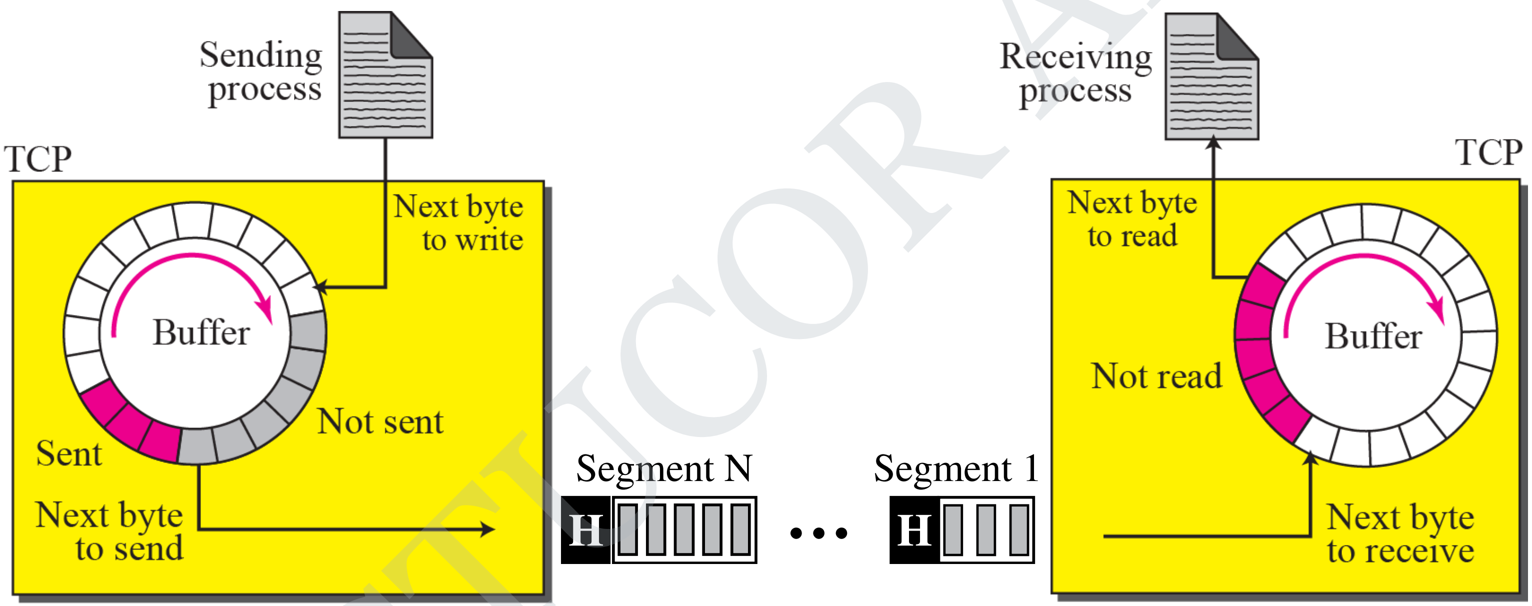
Stream delivery



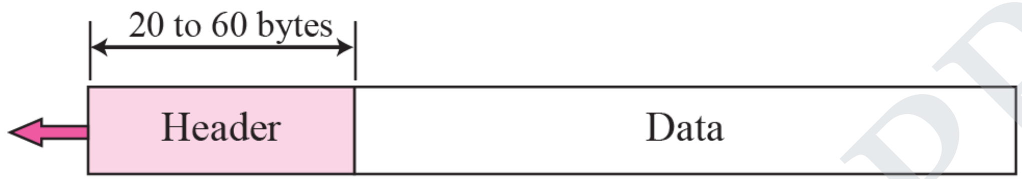
Sending and receiving buffers



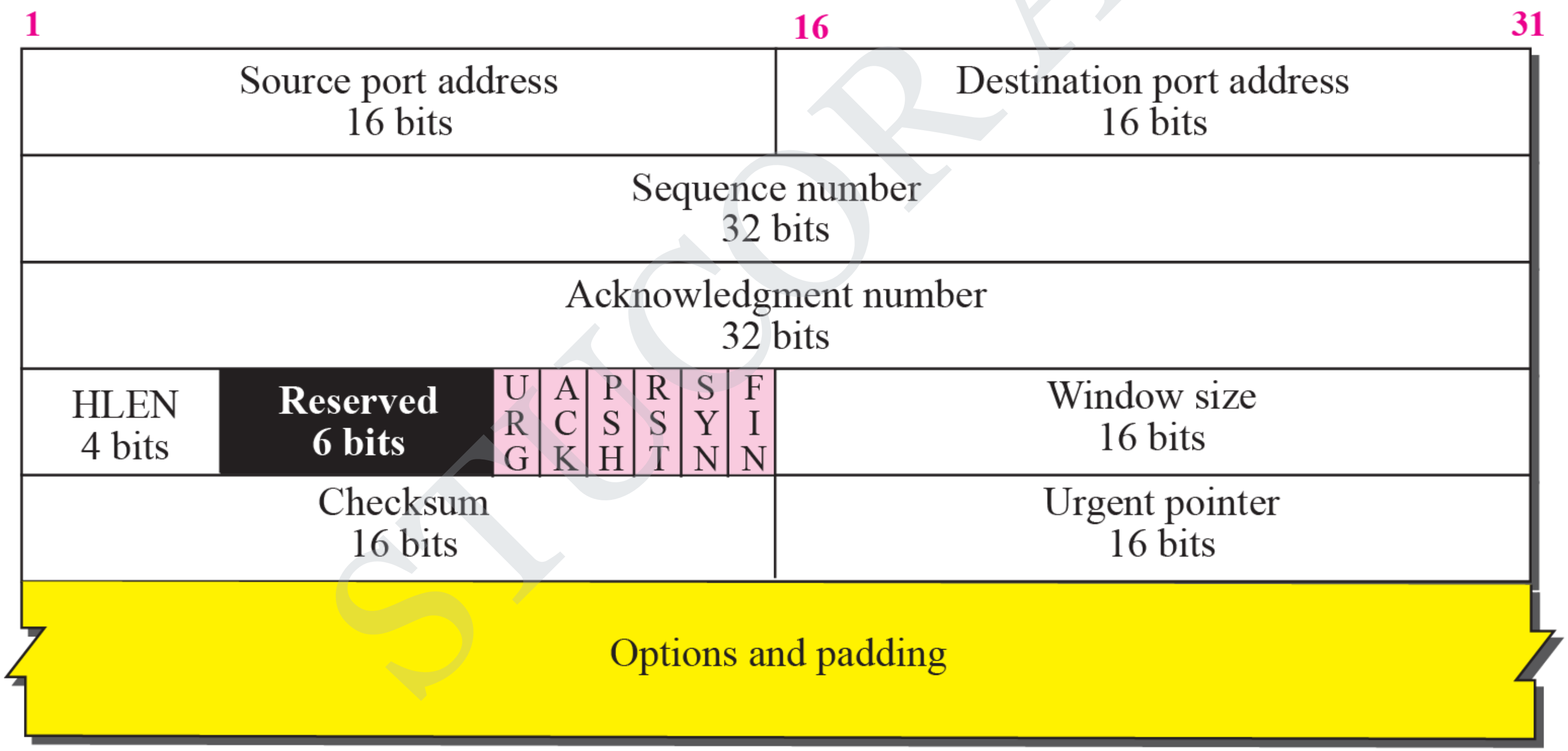
TCP segments



TCP segment format



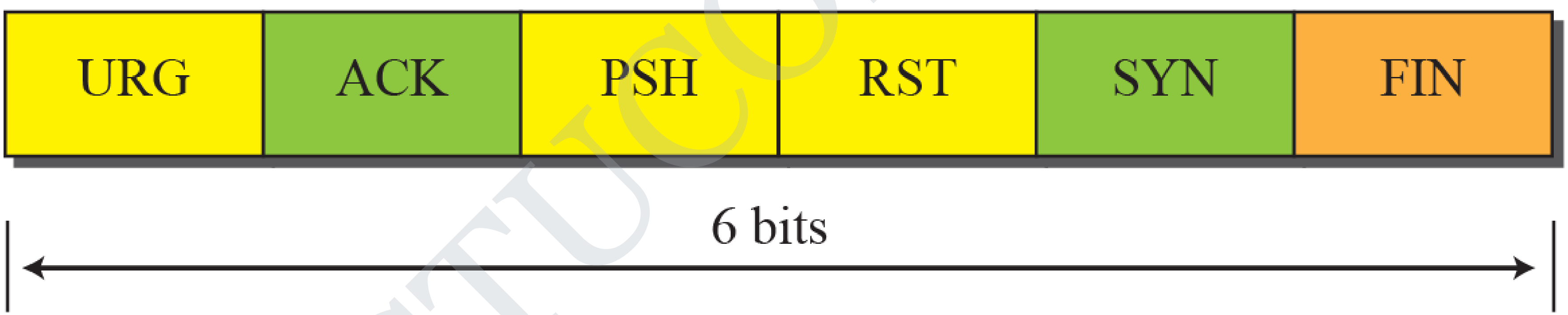
a. Segment



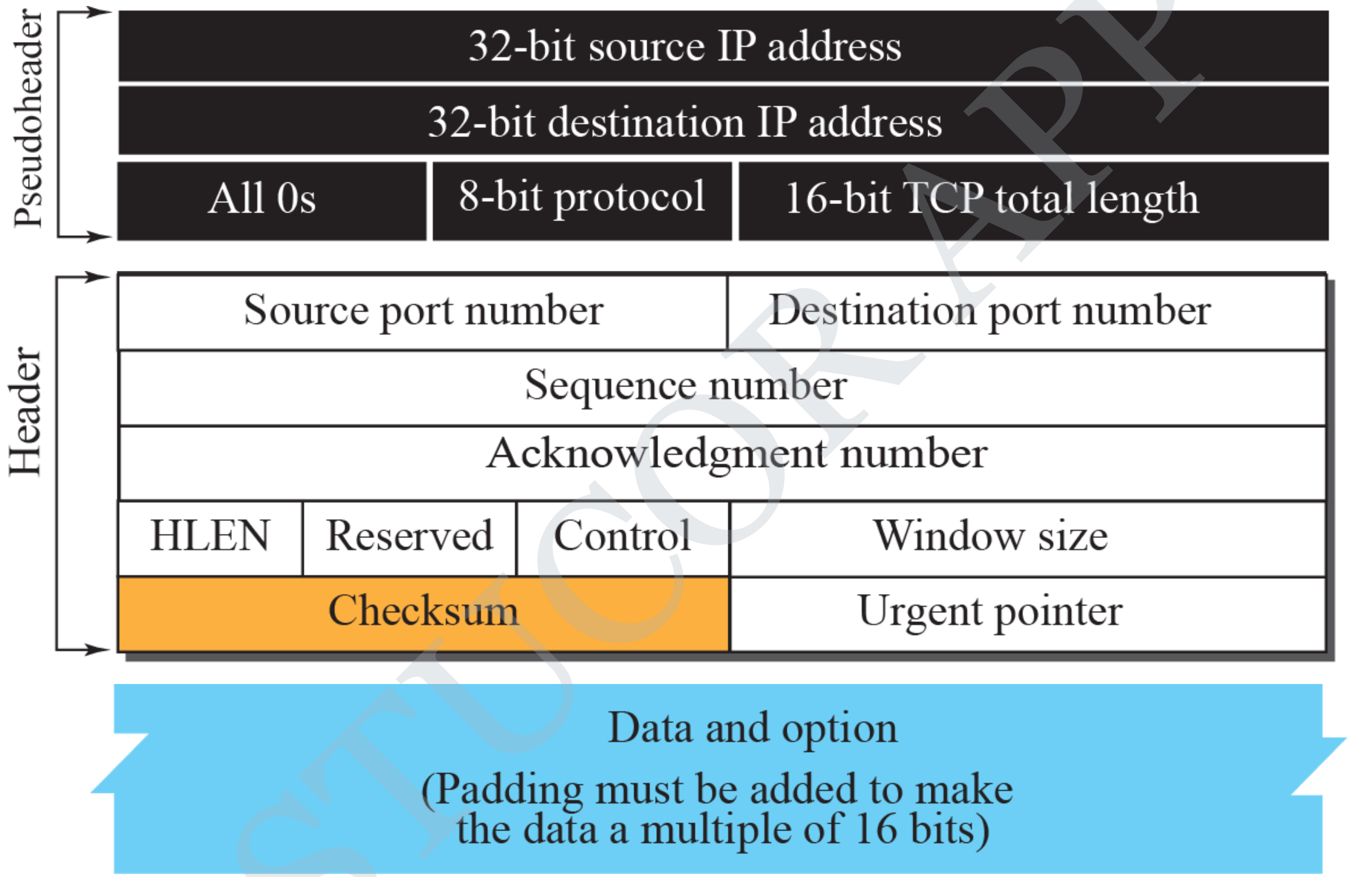
b. Header

Control field

URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection



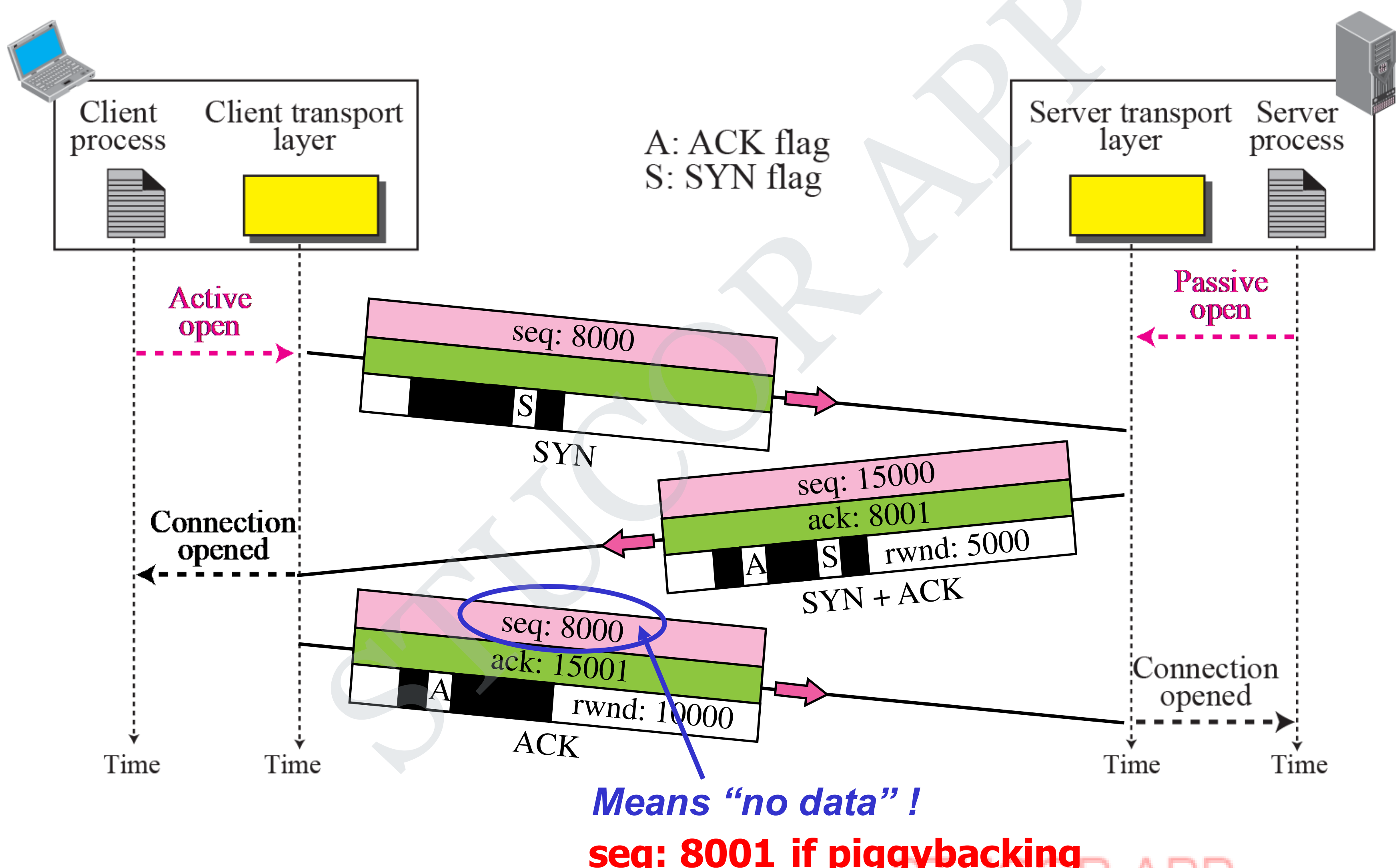
Pseudoheader added to the TCP segment



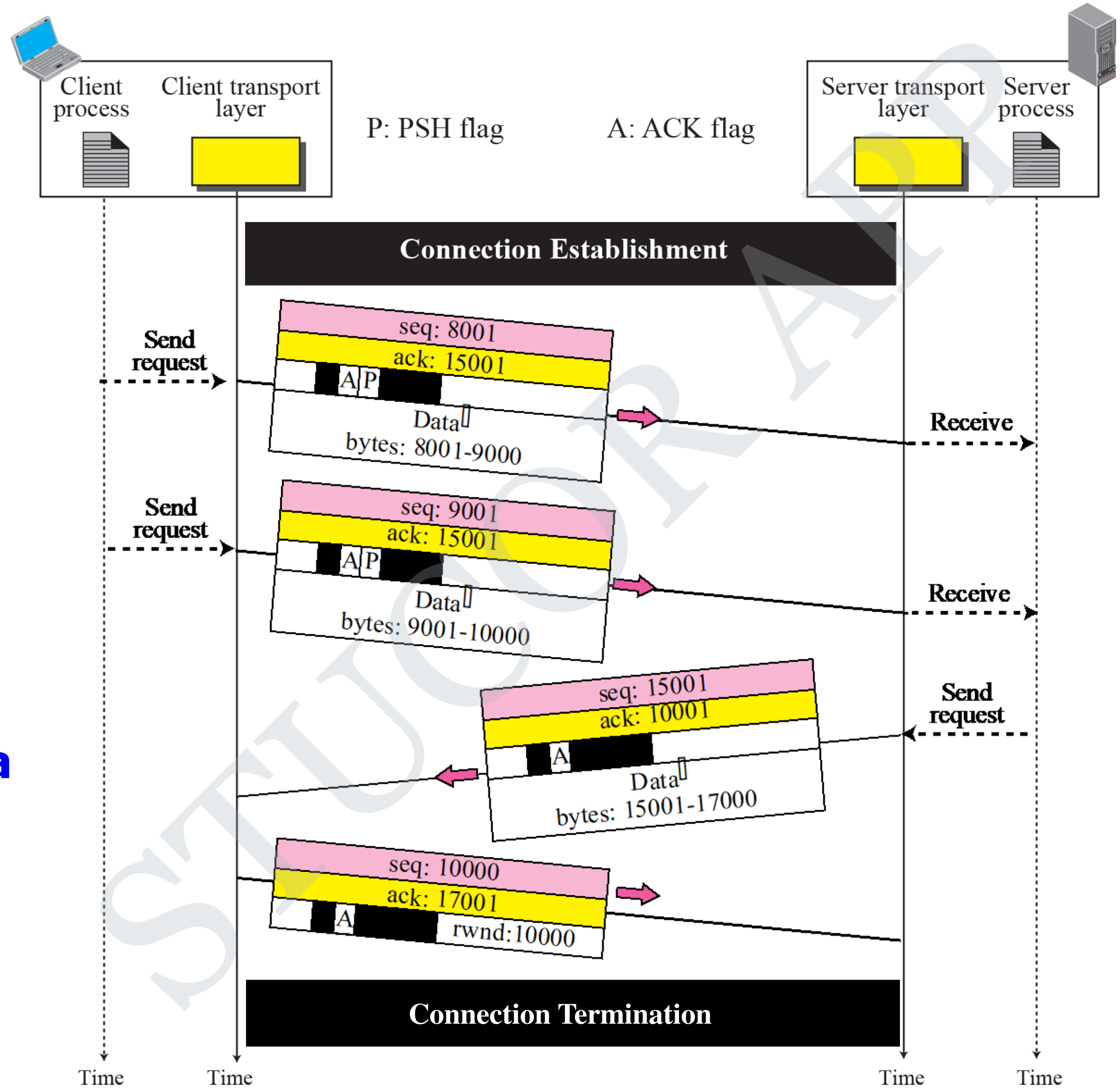
A TCP CONNECTION

TCP is connection-oriented. It establishes a virtual path between the source and destination. All of the segments belonging to a message are then sent over this virtual path. You may wonder how TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted.

Connection establishment using three-way handshake



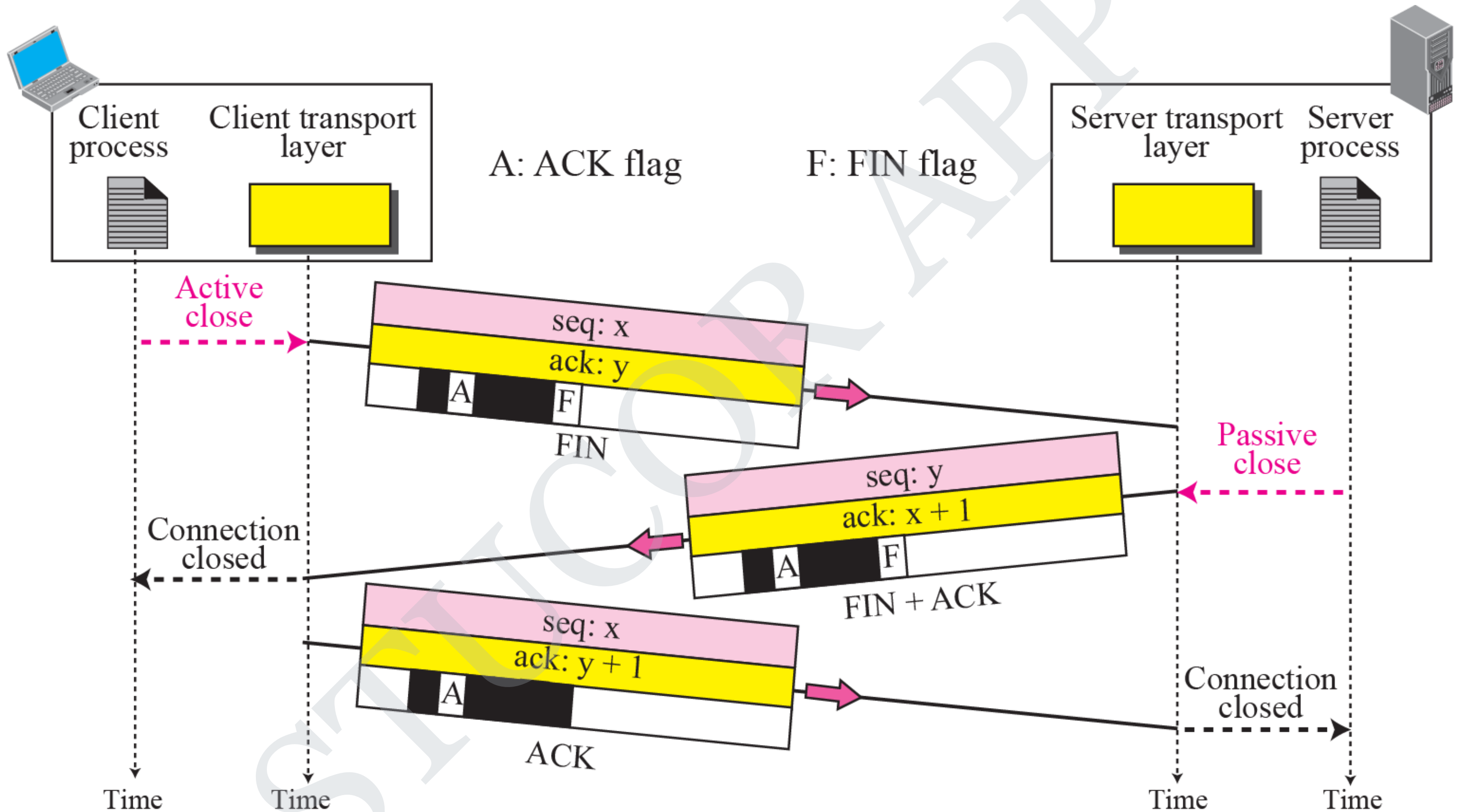
Data Transfer



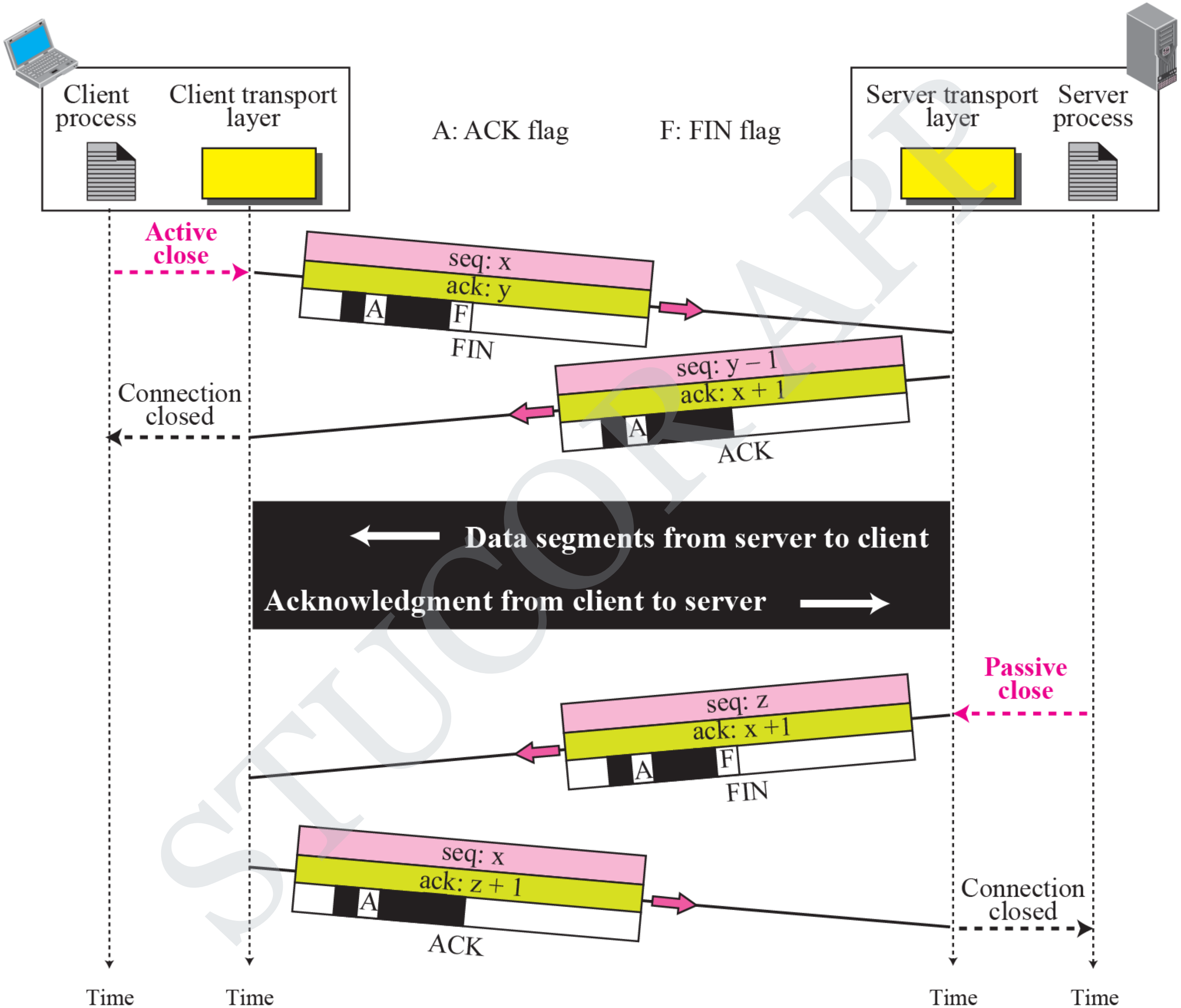
Pushing data

Urgent data

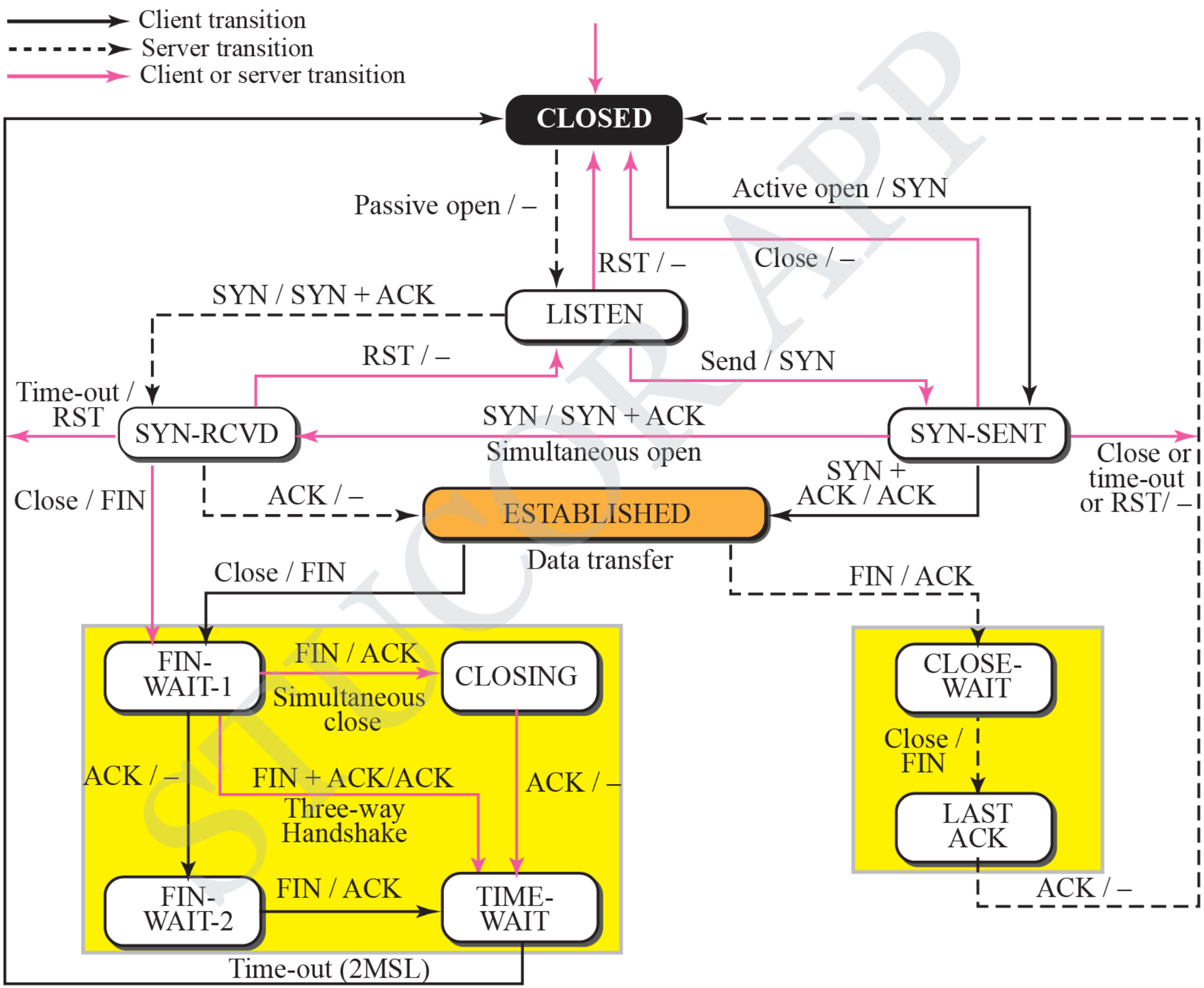
Connection termination using three-way handshake



Half-Close


Client process
Client transport layer
A: ACK flag
F: FIN flag
Server transport layer
Server process
Active close
seq: x
ack: y
A
F
FIN
seq: y – 1
ack: x + 1
A
ACK
Connection closed
Data segments from server to client
Acknowledgment from client to server
Passive close
seq: z
ack: x +1
A
F
FIN
seq: x
ack: z + 1
A
ACK
Connection closed
Time
Time
Time
Time

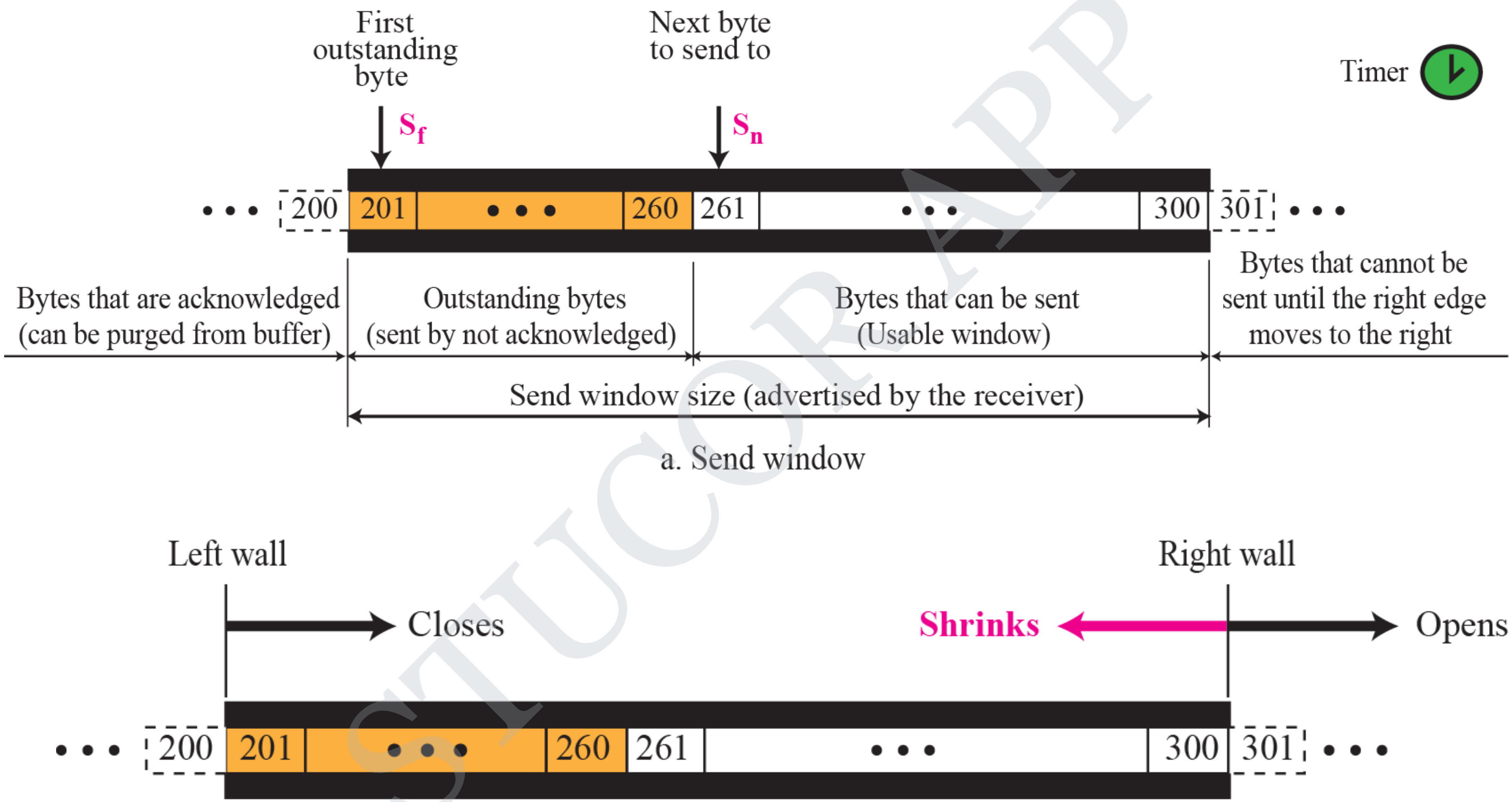
State transition diagram



WINDOWS IN TCP

Before discussing data transfer in TCP and the issues such as flow, error, and congestion control, we describe the windows used in TCP. TCP uses two windows (send window and receive window) for each direction of data transfer, which means four windows for a bidirectional communication. To make the discussion simple, we make an assumption that communication is only unidirectional; the bidirectional communication can be inferred using two unidirectional communications with piggybacking.

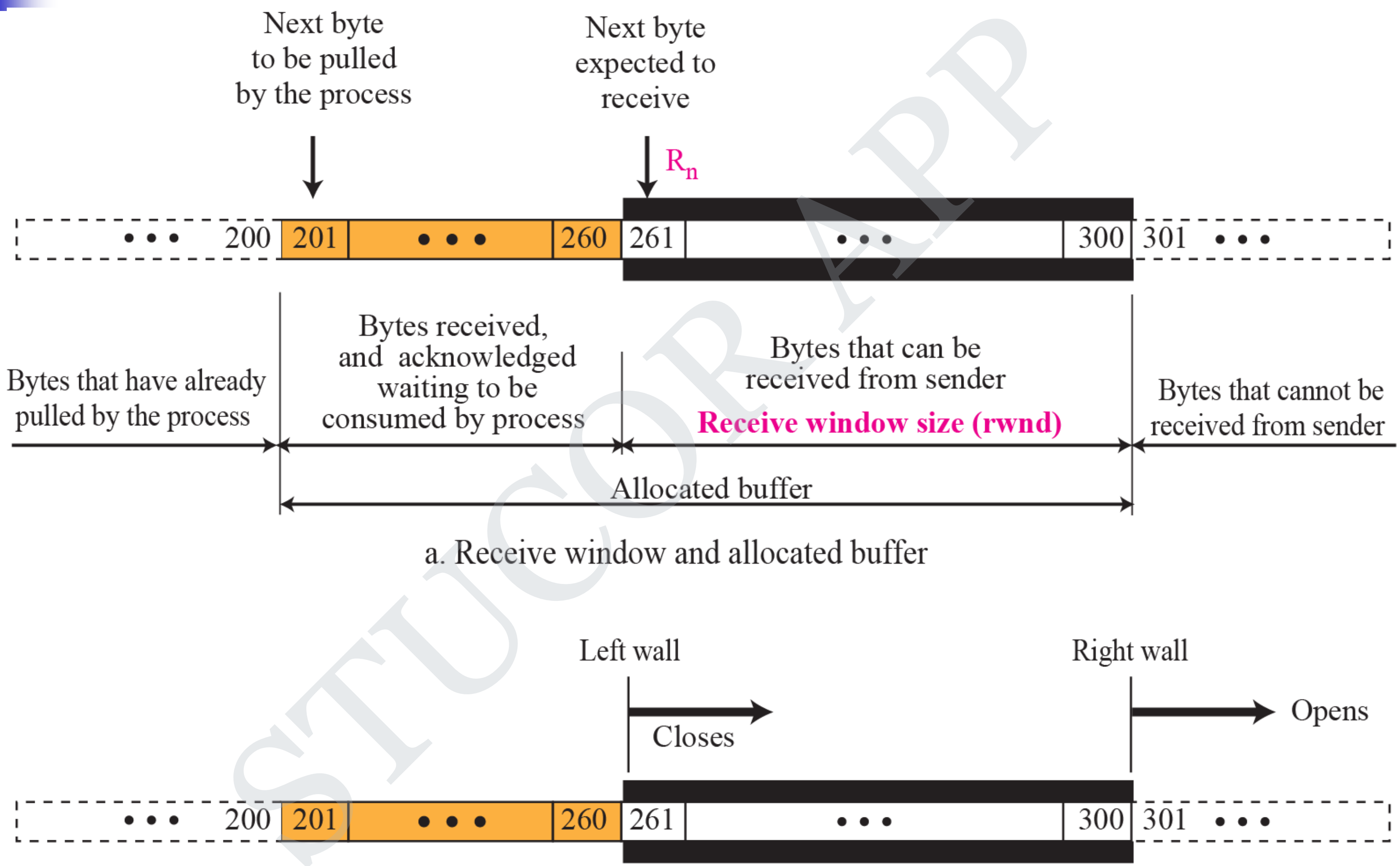
Send window in TCP



a. Send window

b. Opening, closing, and shrinking send window

Receive window in TCP



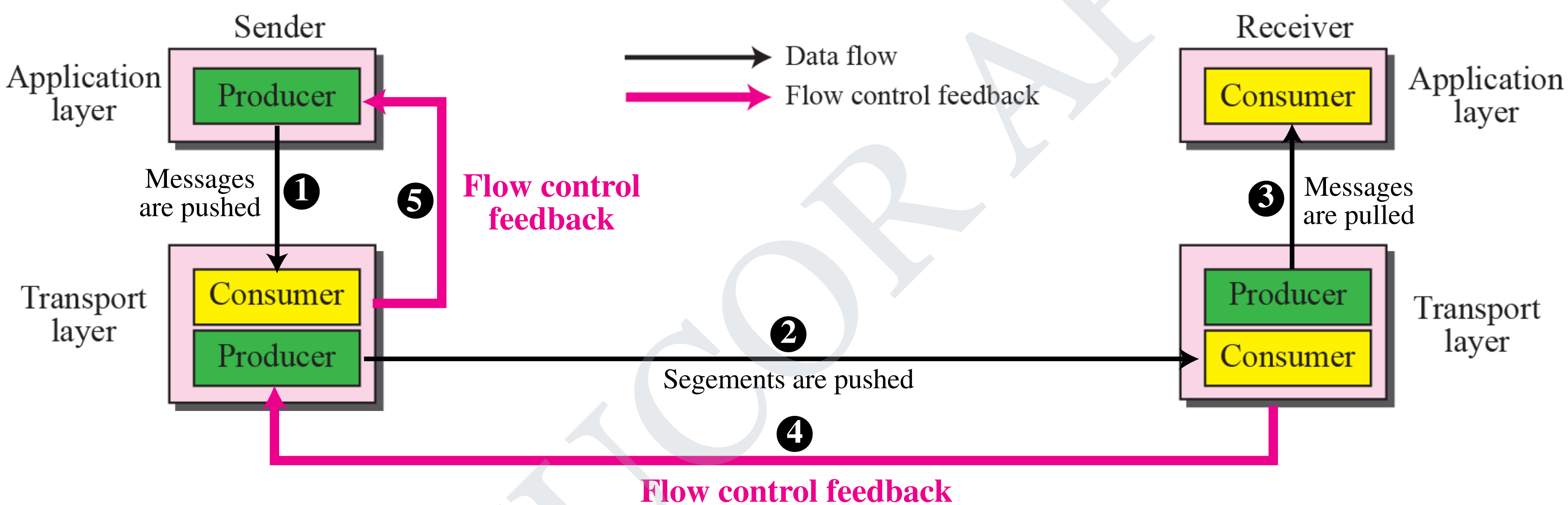
a. Receive window and allocated buffer

b. Opening and closing of receive window

FLOW CONTROL

As discussed in Chapter 13, flow control balances the rate a producer creates data with the rate a consumer can use the data. TCP separates flow control from error control. In this section we discuss flow control, ignoring error control. We temporarily assume that the logical channel between the sending and receiving TCP is error-free. Figure 15.24 shows unidirectional data transfer between a sender and a receiver; bidirectional data transfer can be deduced from unidirectional one as discussed in Chapter 13.

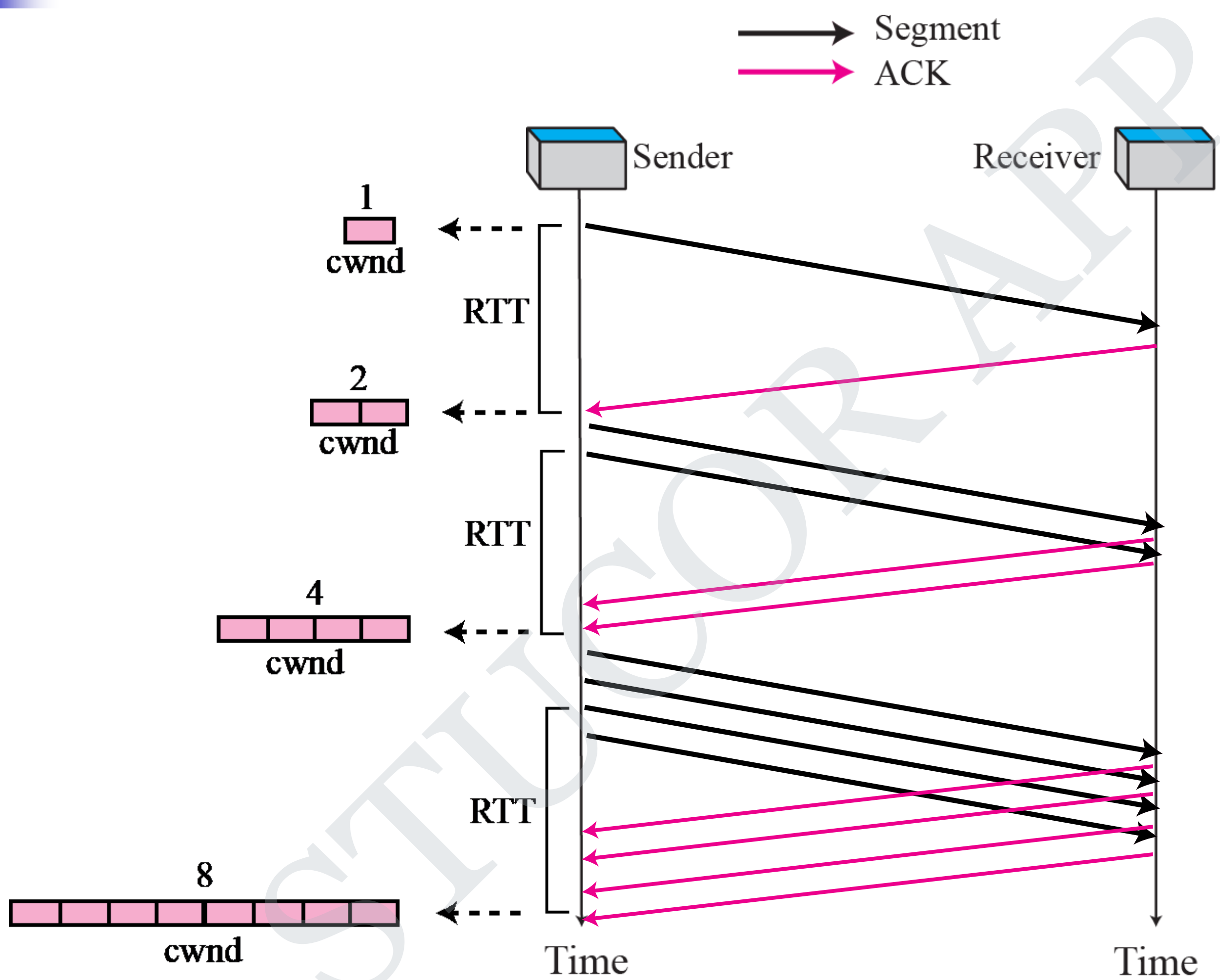
TCP/IP protocol suite



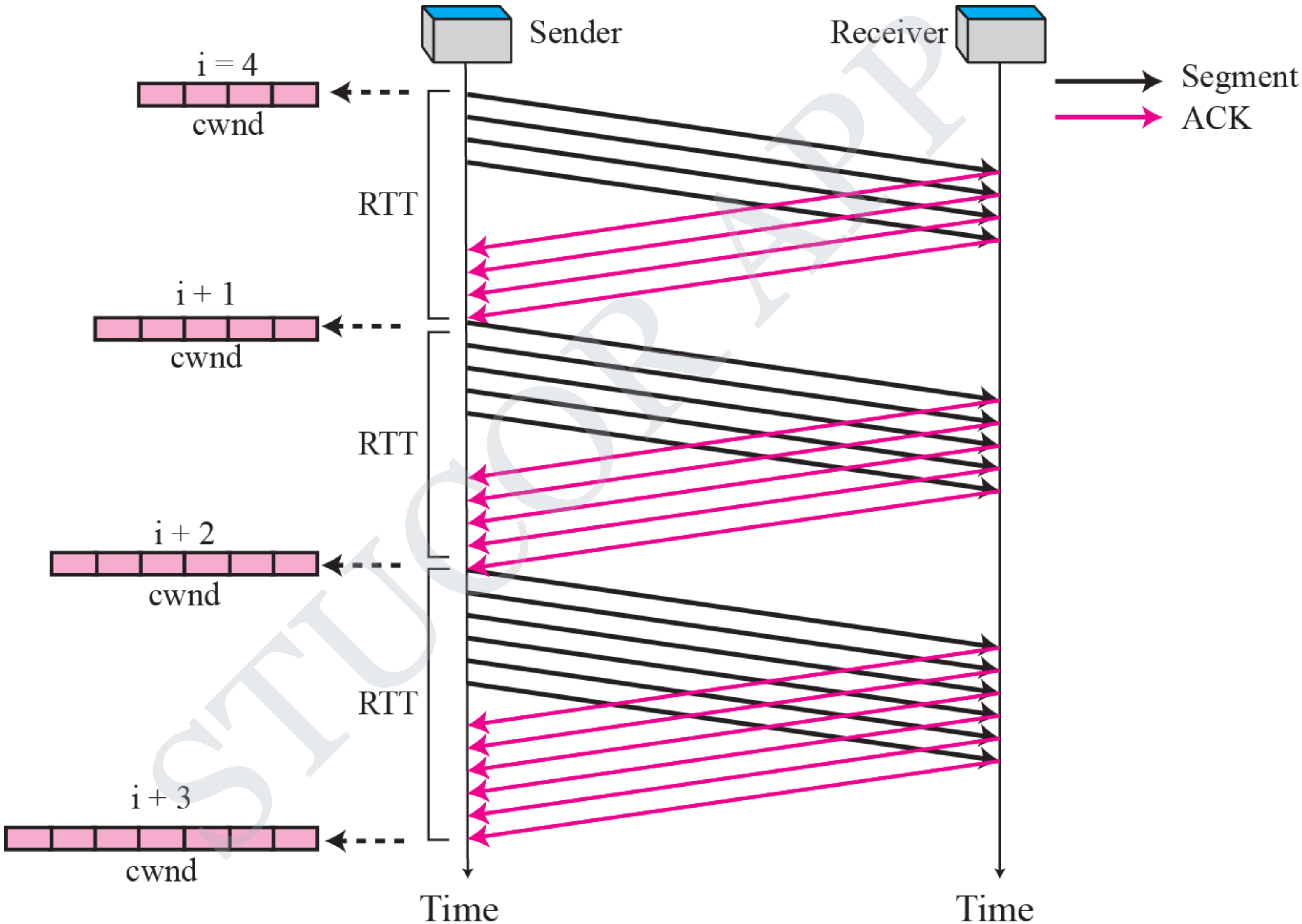
CONGESTION CONTROL

Congestion control in TCP is based on both open loop and closed-loop mechanisms. TCP uses a congestion window and a congestion policy that avoid congestion and detect and alleviate congestion after it has occurred.

Slow start, exponential increase



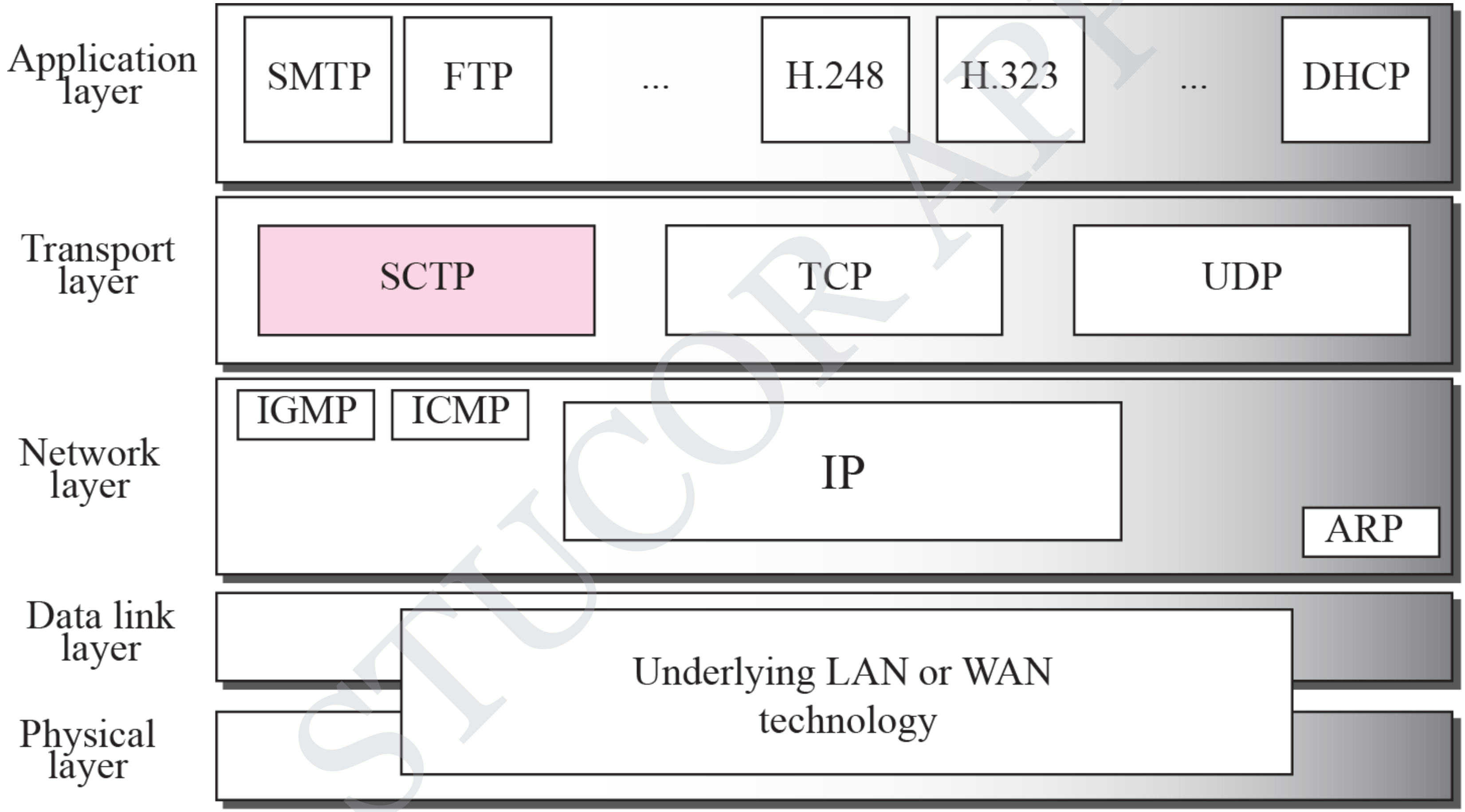
Congestion avoidance, additive increase



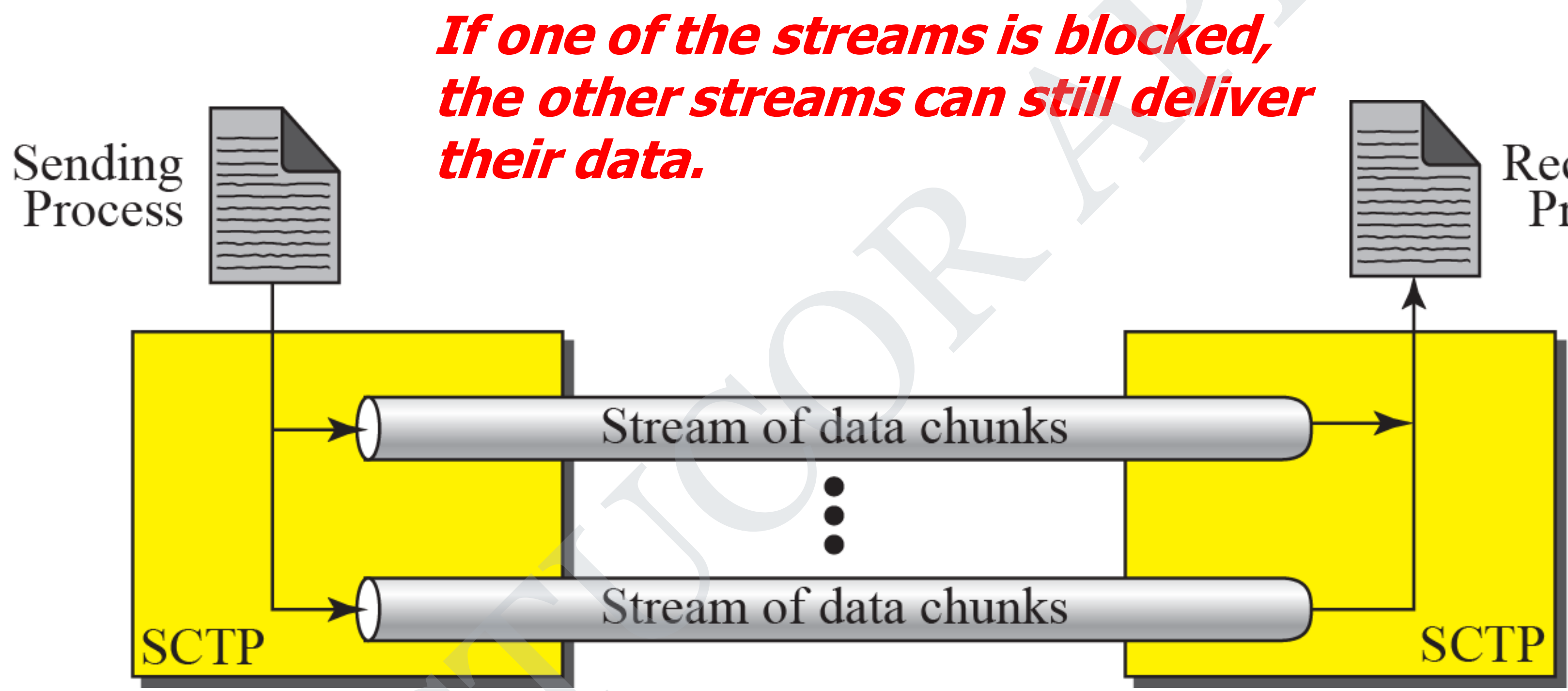
SCTP

Stream Control Transmission Protocol (SCTP) is a new reliable, message-oriented transport-layer protocol. SCTP lies between the application layer and the network layer and serves as the intermediary between the application programs and the network operations.

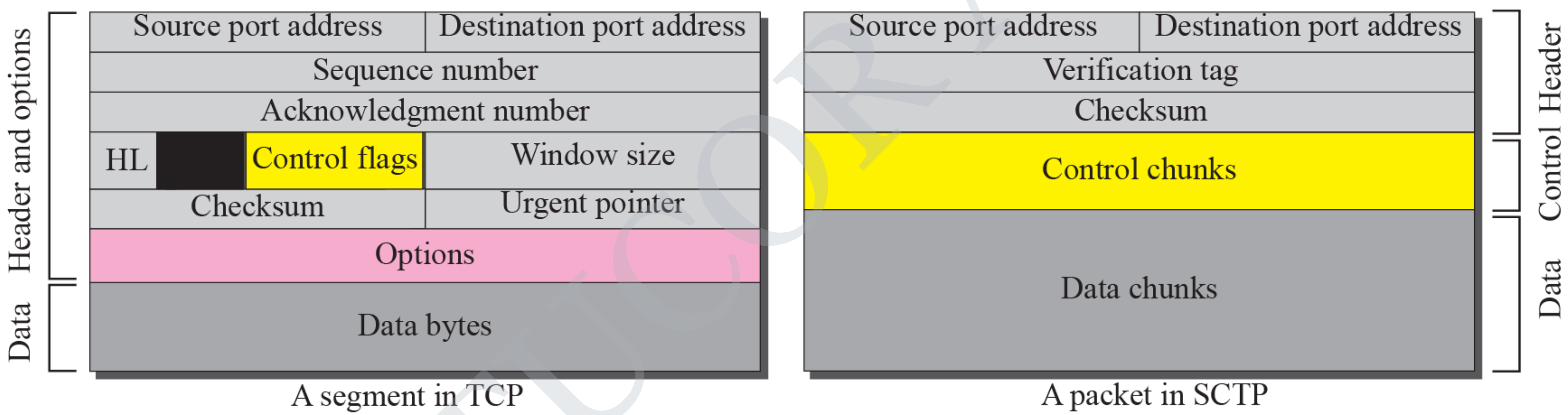
TCP/IP Protocol suite



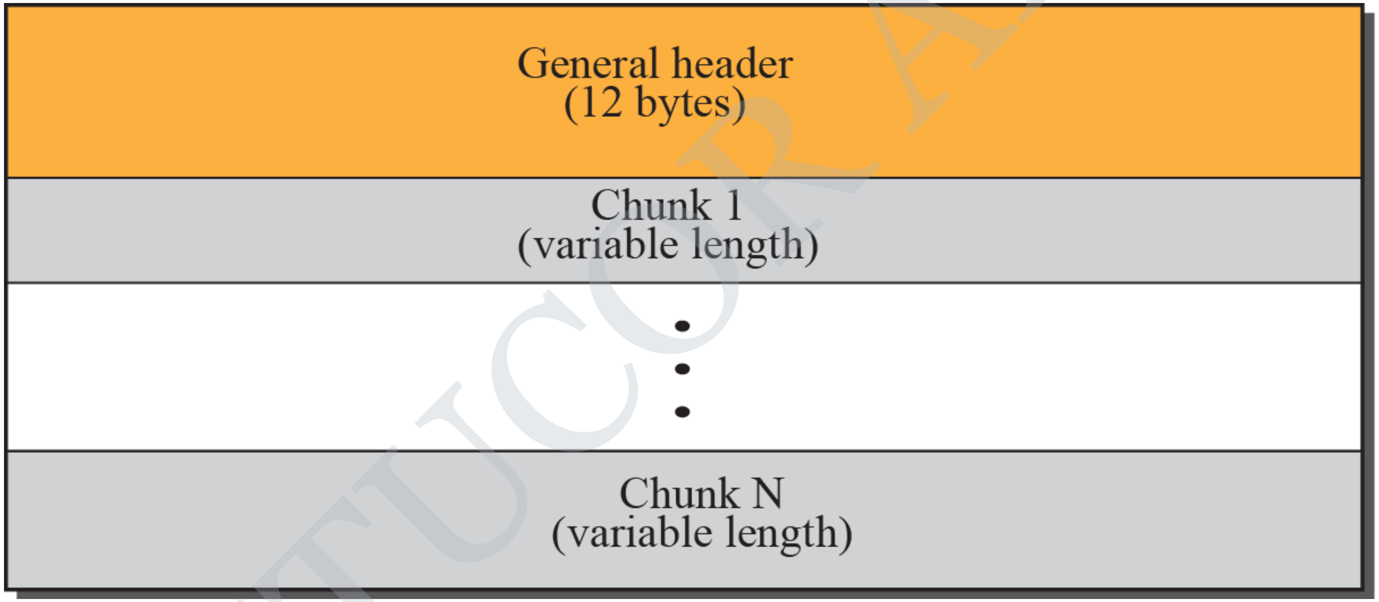
Multiple-stream concept



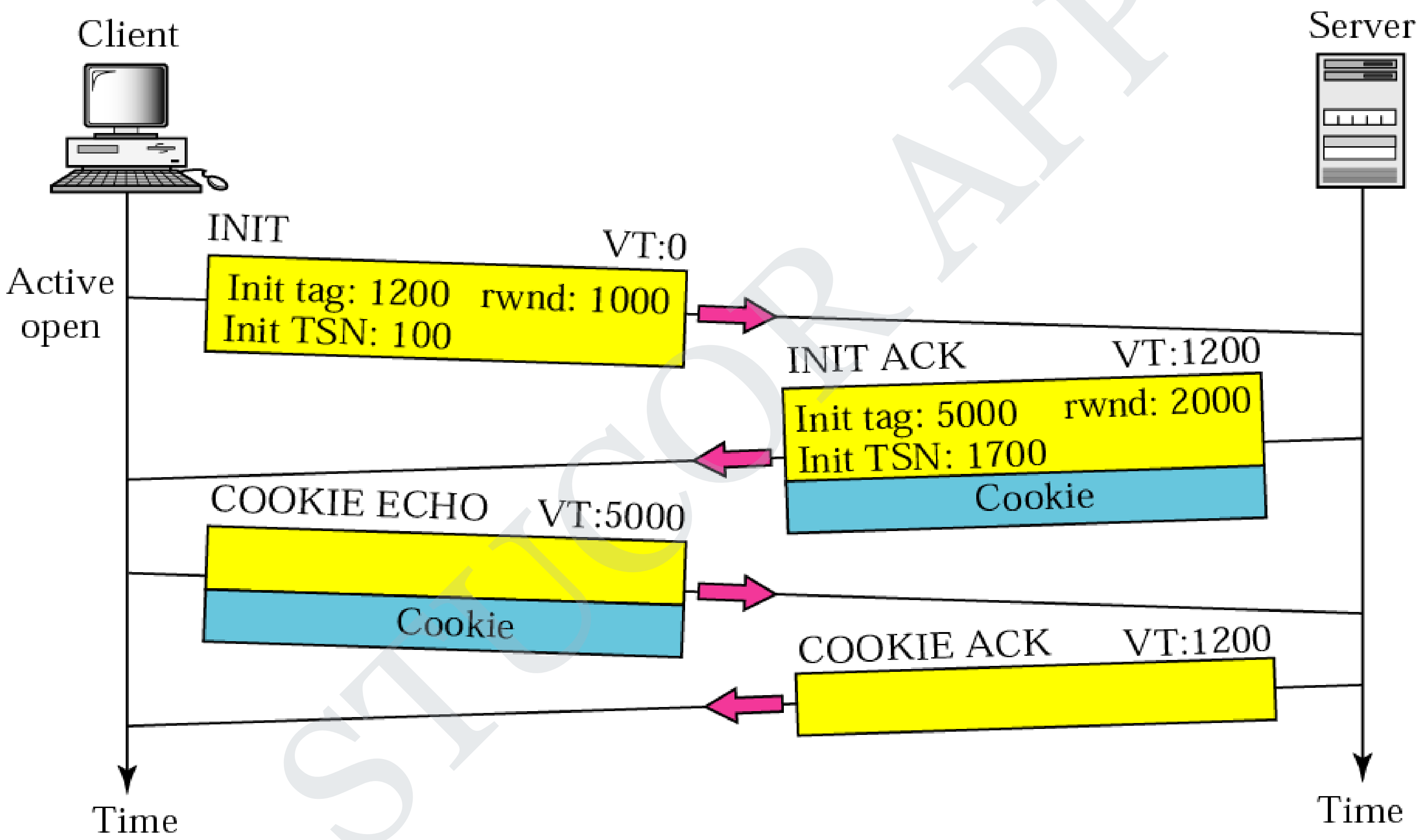
Comparison between a TCP segment and an SCTP packet



SCTP packet format



Four-way handshaking



CS8591 – COMPUTER NETWORKS

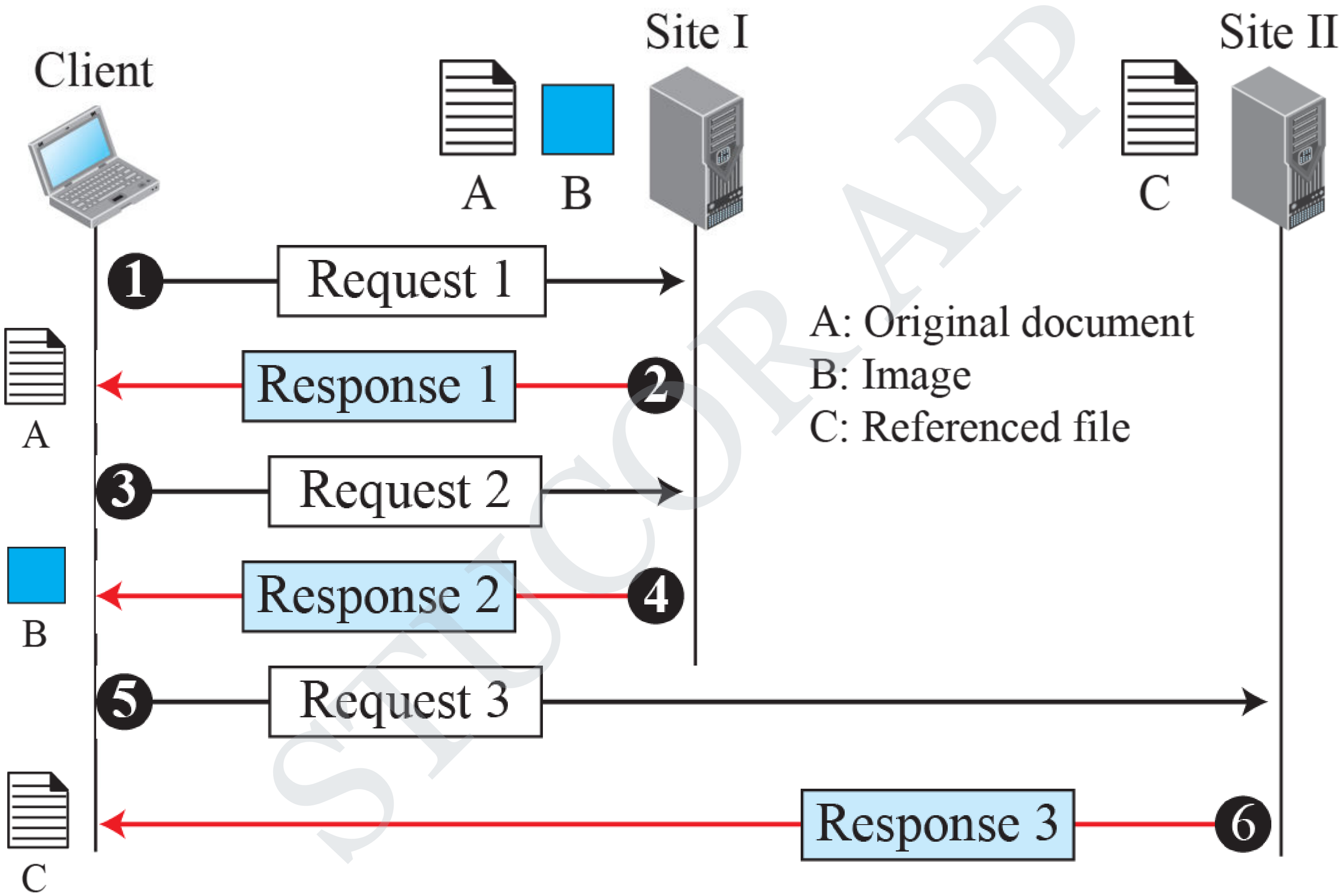
UNIT –V

Dr.R.SASIKUMAR
Professor/CSE
R.M.D.Engineering College

APPLICATION LAYER

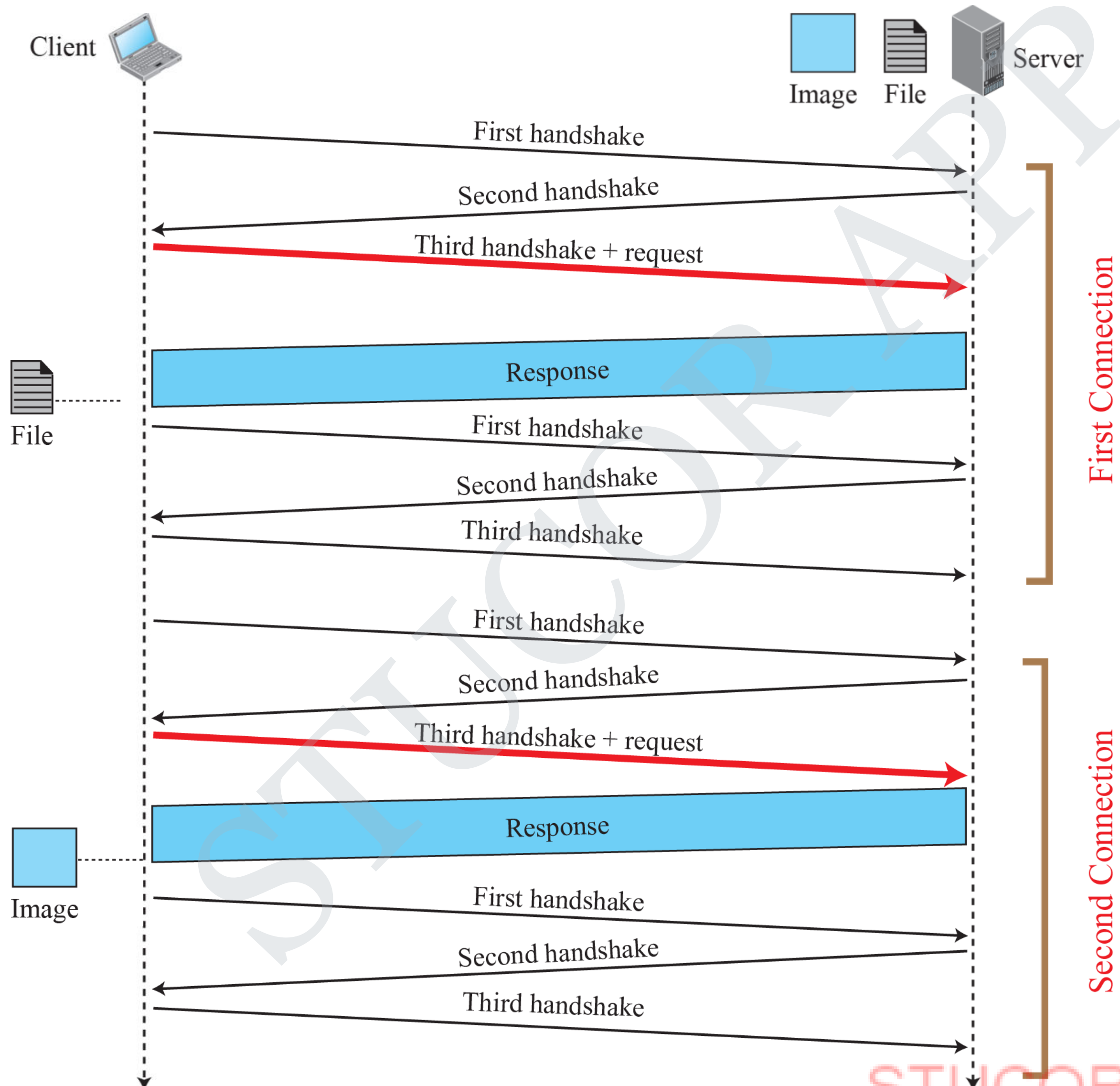
World Wide Web

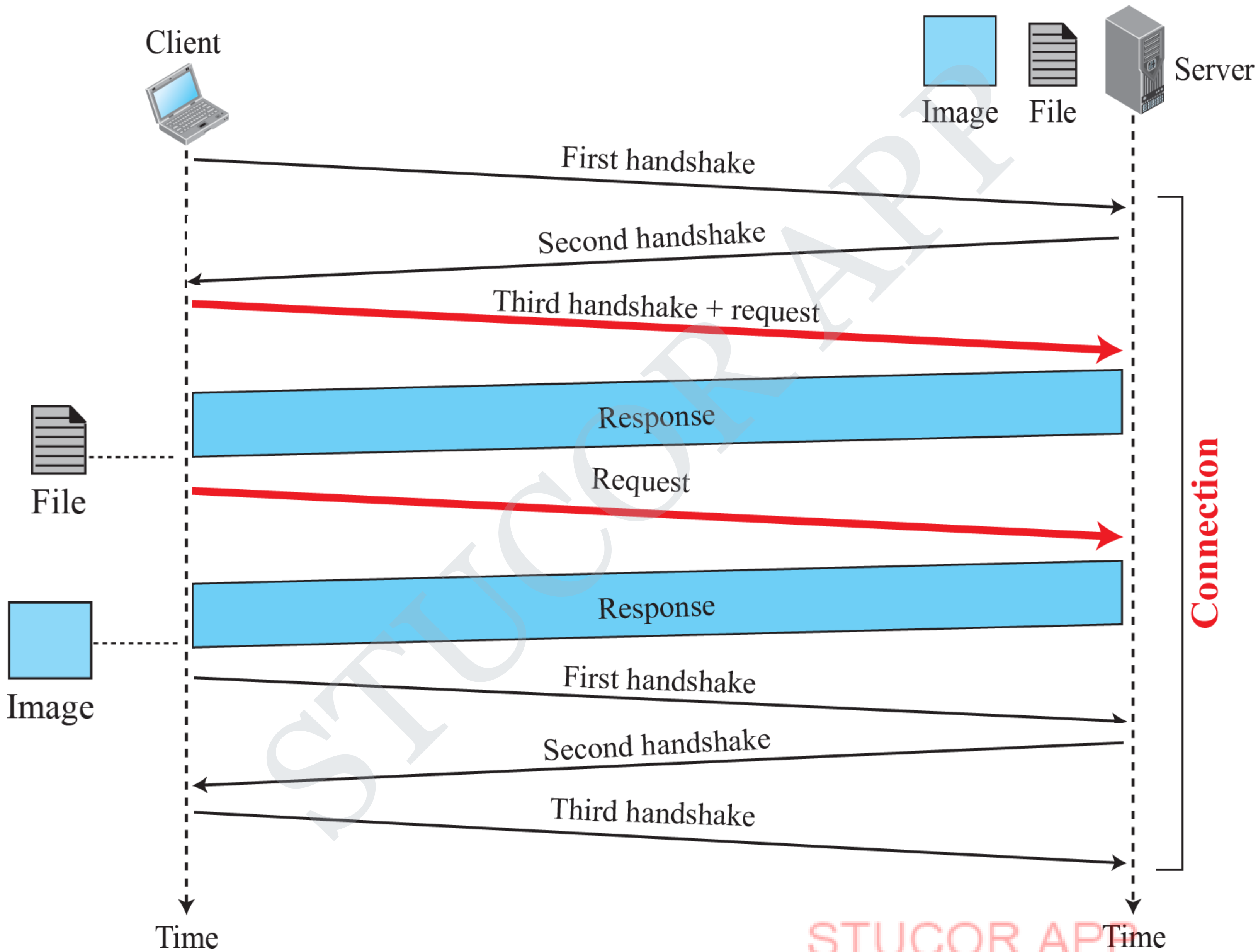
The idea of the Web was first proposed by Tim Berners-Lee in 1989 at CERN, the European Organization for Nuclear Research, to allow several researchers at different locations throughout Europe to access each others' researches. The commercial Web started in the early 1990s.


Site I
Site II
Client
A
B
C
Request 1
Response 1
Request 2
Response 2
Request 3
Response 3
A: Original document
B: Image
C: Referenced file
1
2
3
4
5
6

HyperText Transfer Protocol

The HyperText Transfer Protocol (HTTP) is used to define how the client-server programs can be written to retrieve web pages from the Web. An HTTP client sends a request; an HTTP server returns a response. The server uses the port number 80; the client uses a temporary port number. HTTP uses the services of TCP, which, as discussed before, is a connection-oriented and reliable protocol.


Client
Image
File
Server
First handshake
Second handshake
Third handshake + request
Response
File
First handshake
Second handshake
Third handshake
First Connection
First handshake
Second handshake
Third handshake + request
Response
Image
First handshake
Second handshake
Third handshake
Second Connection


Client
Image
File
Server
First handshake
Second handshake
Third handshake + request
Response
File
Request
Response
Image
First handshake
Second handshake
Third handshake
Connection
Time
Time

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
PUT	Sends a document from the client to the server
POST	Sends some information from the client to the server
TRACE	Echoes the incoming request
DELETE	Removes the web page
CONNECT	Reserved
OPTIONS	Inquires about available options

Request Header Names

Header	*Description*
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server (explained later)
If-Modified-Since	If the file is modified since a specific date

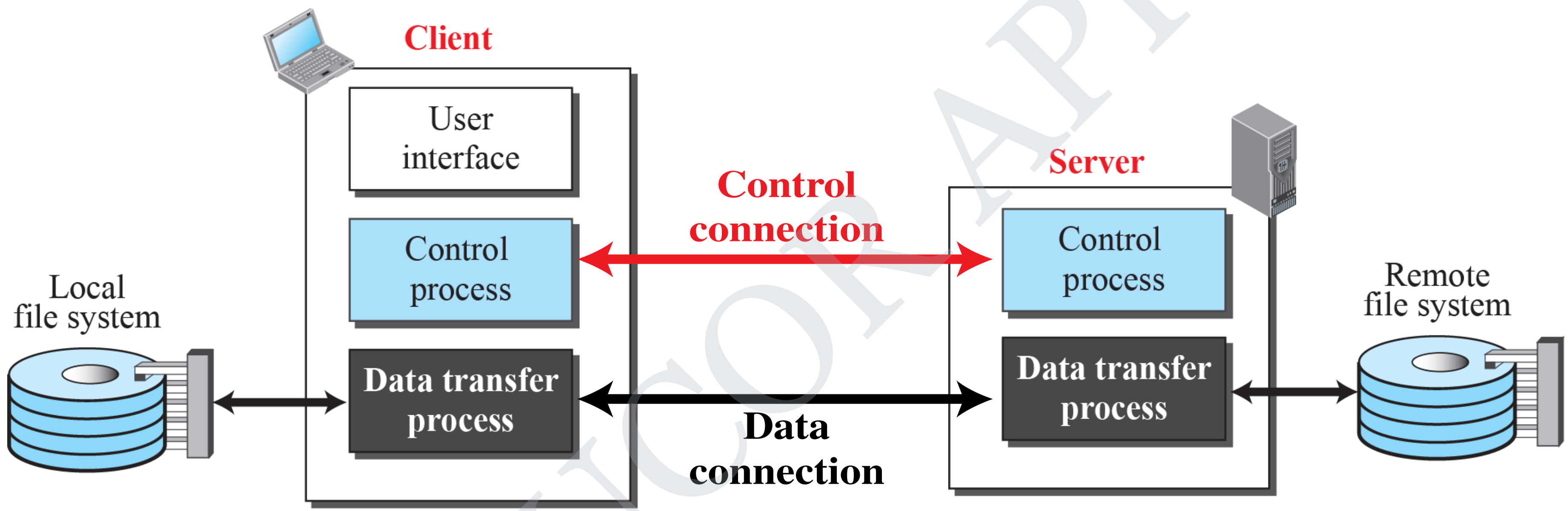
Response Header Names

Header	*Description*
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change

FTP

File Transfer Protocol (FTP) is the standard protocol provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.

FTP


Client
User interface
Control process
Data transfer process
Control connection
Data connection
Server
Control process
Data transfer process
Local file system
Remote file system

Two Connections

The two connections in FTP have different lifetimes. The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transfer activity. It opens each time commands that involve transferring files are used, and it closes when the file is transferred.

Control Connection

For control communication, FTP uses the same approach as TELNET (discussed later). It uses the NVT ASCII character set as used by TELNET. Communication is achieved through commands and responses. This simple method is adequate for the control connection because we send one command (or response) at a time. Each line is terminated with a two-character (carriage return and line feed) end-of-line token.

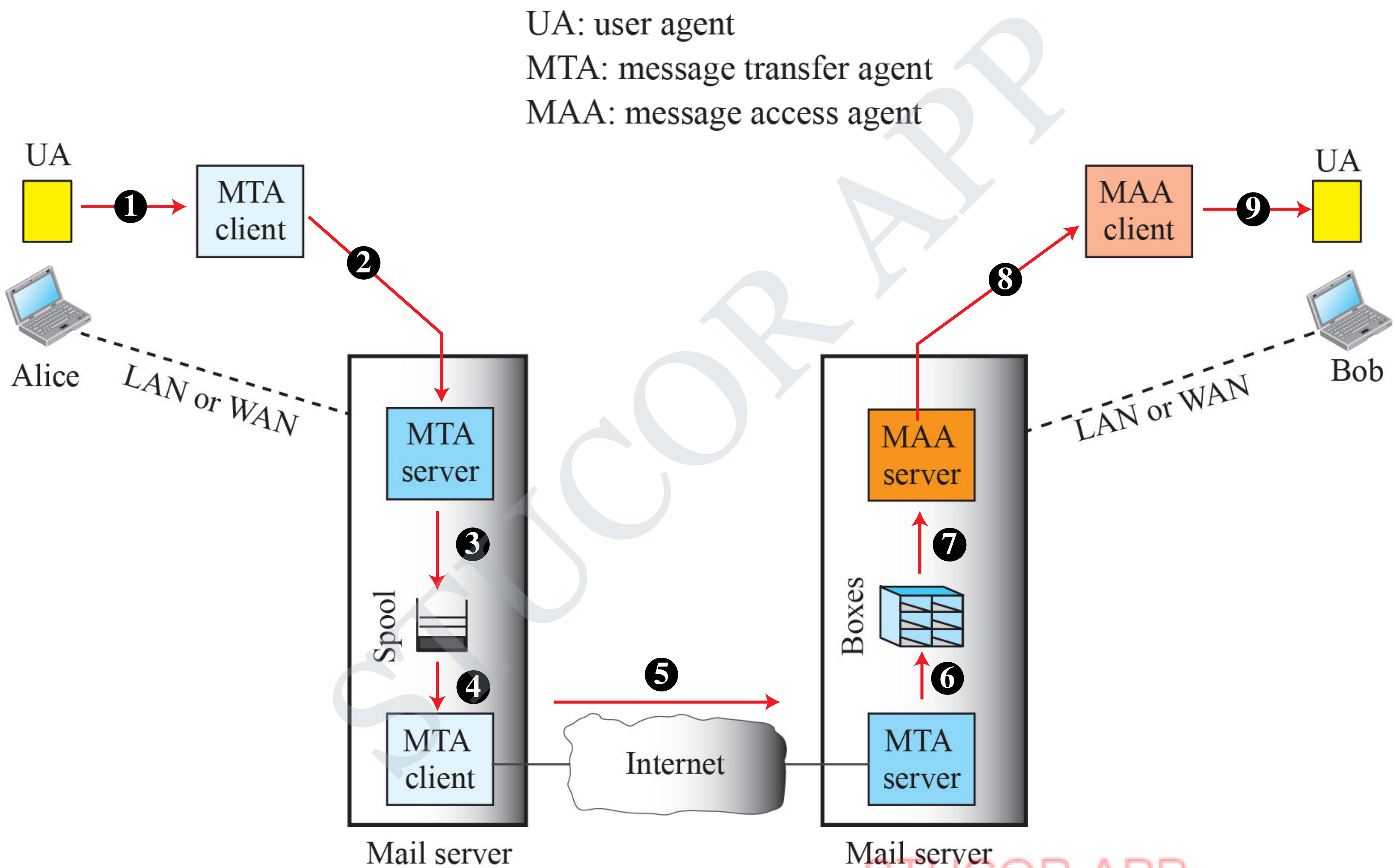
Some FTP commands

Command	*Argument(s)*	*Description*
ABOR		Abort the previous command
CDUP		Change to parent directory
CWD	Directory name	Change to another directory
DELE	File name	Delete a file
LIST	Directory name	List subdirectories or files
MKD	Directory name	Create a new directory
PASS	User password	Password
PASV		Server chooses a port
PORT	port identifier	Client chooses a port
PWD		Display name of current directory
QUIT		Log out of the system
RETR	File name(s)	Retrieve files; files are transferred from server to client
RMD	Directory name	Delete a directory
RNFR	File name (old)	Identify a file to be renamed

ELECTRONIC MAIL

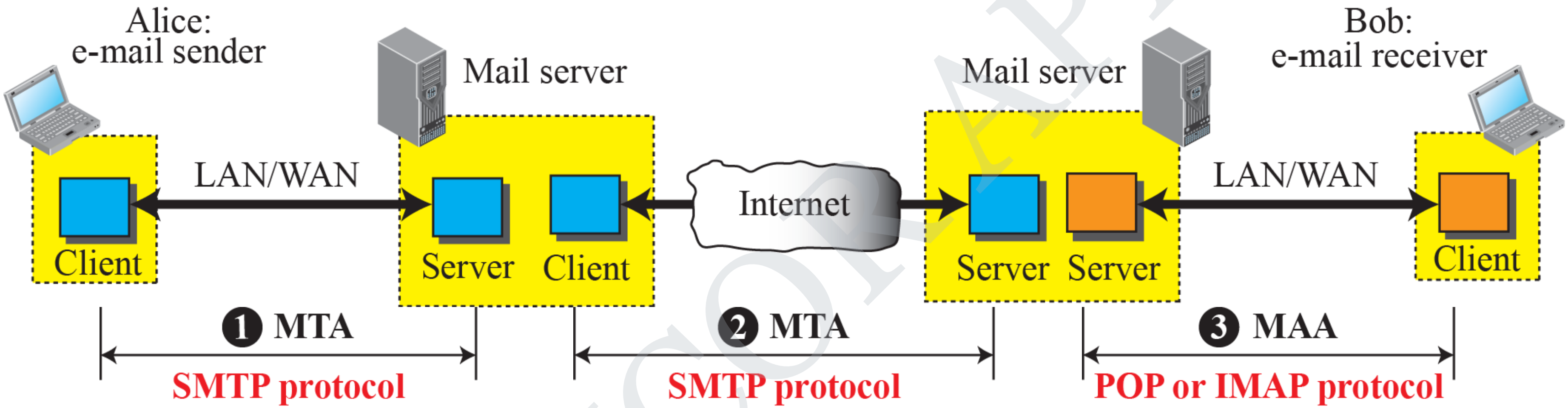
Electronic mail (or e-mail) allows users to exchange messages. The nature of this application is different from other applications discussed so far. This means that the idea of client/server programming should be implemented in another way: using some intermediate computers (servers).

Common scenario



E-mail address

Protocols used in electronic mail



SMTP Commands

Keyword	*Argument(s)*	*Description*
HELO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies the sender of the message
RCPT TO	Intended recipient	Identifies the recipient of the message
DATA	Body of the mail	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the status of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list.
HELP	Command name	Asks the recipient to send information about the command sent as the argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and not to the mailbox
SMOL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *or* the mailbox of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *and* the mailbox of the recipient

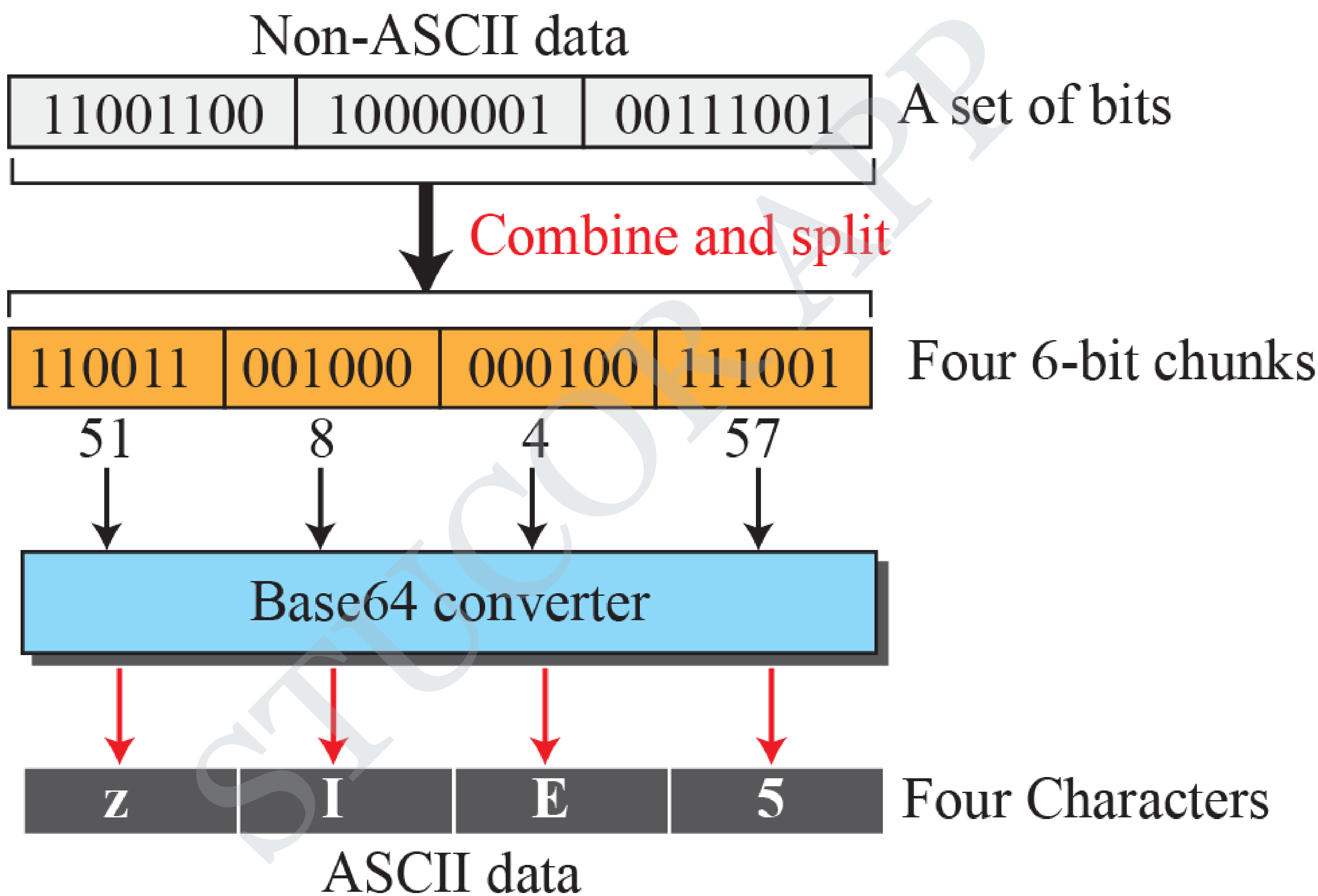
SMTP responses (Continued)

Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage

SMTP responses (continued)

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 temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

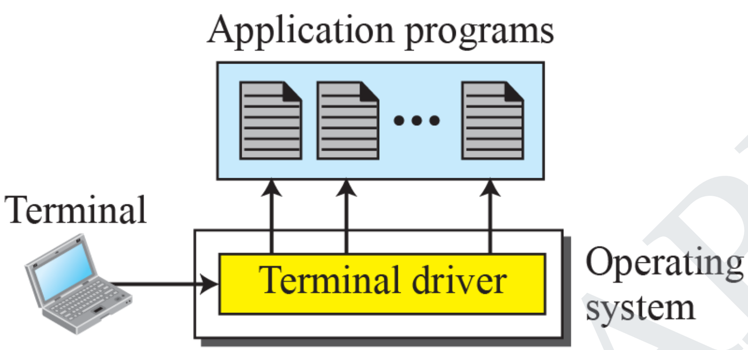
Base64 conversion



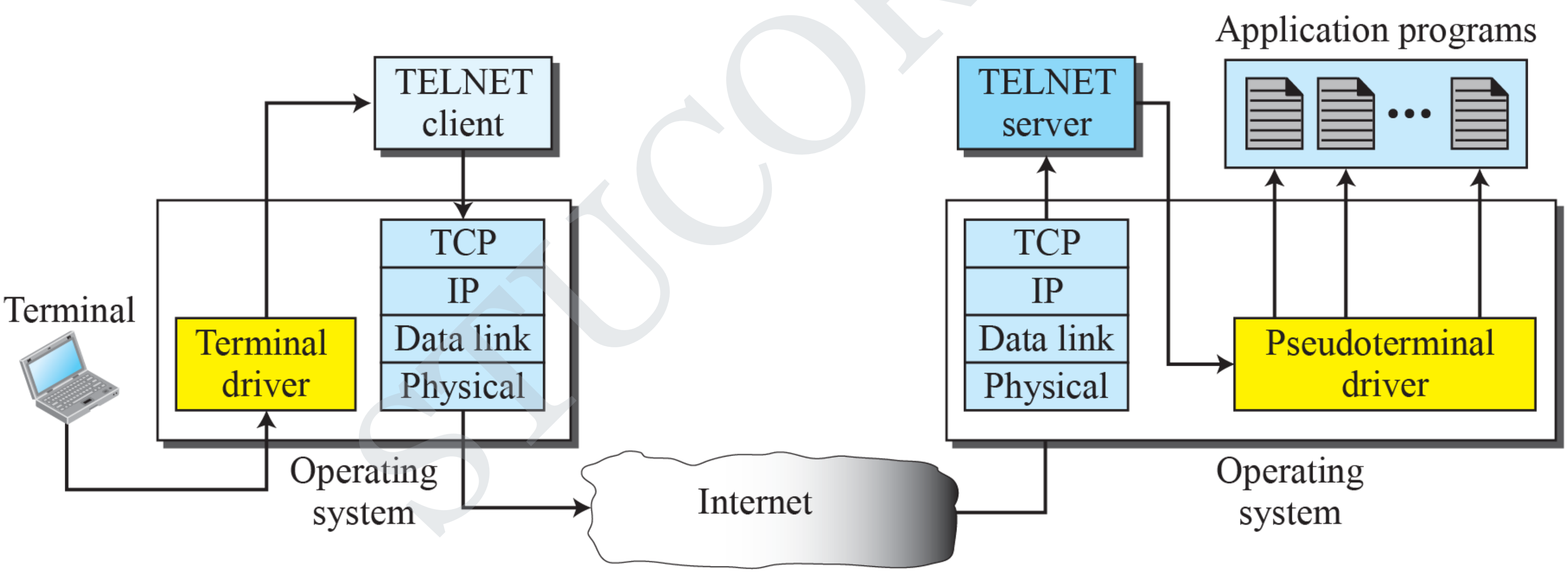
TELNET

It is impossible to have a client/server pair for each type of service we need; the number of servers soon becomes intractable. The idea is not scalable. The solution is to have a specific client/server program for a set of common scenarios, but to have some generic client/server programs for the rest.

Local versus remote logging

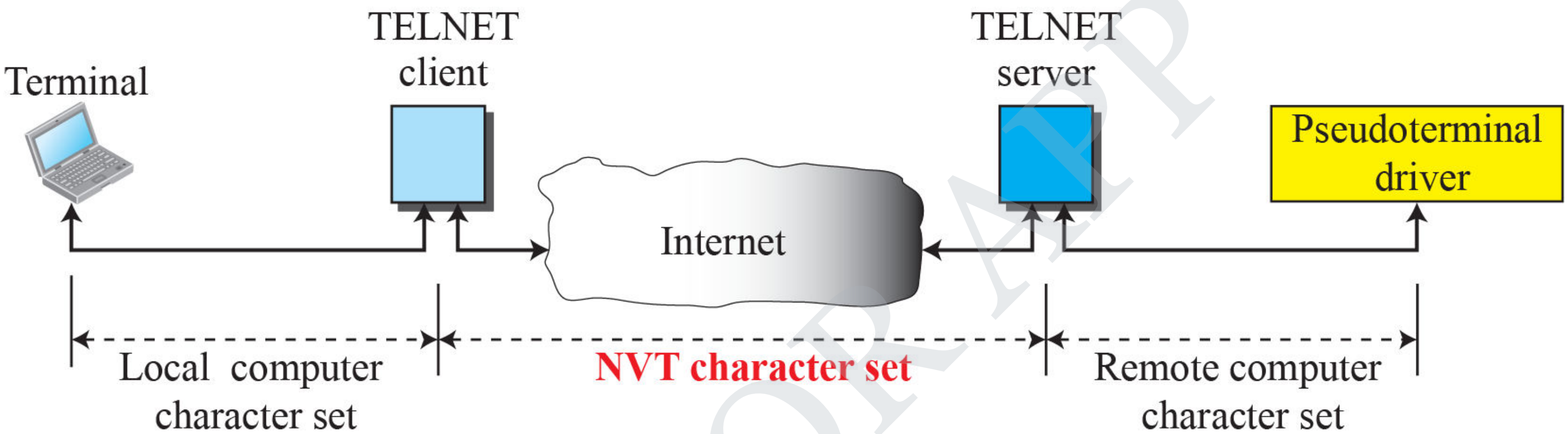


a. Local logging



b. Remote logging

Concept of NVT

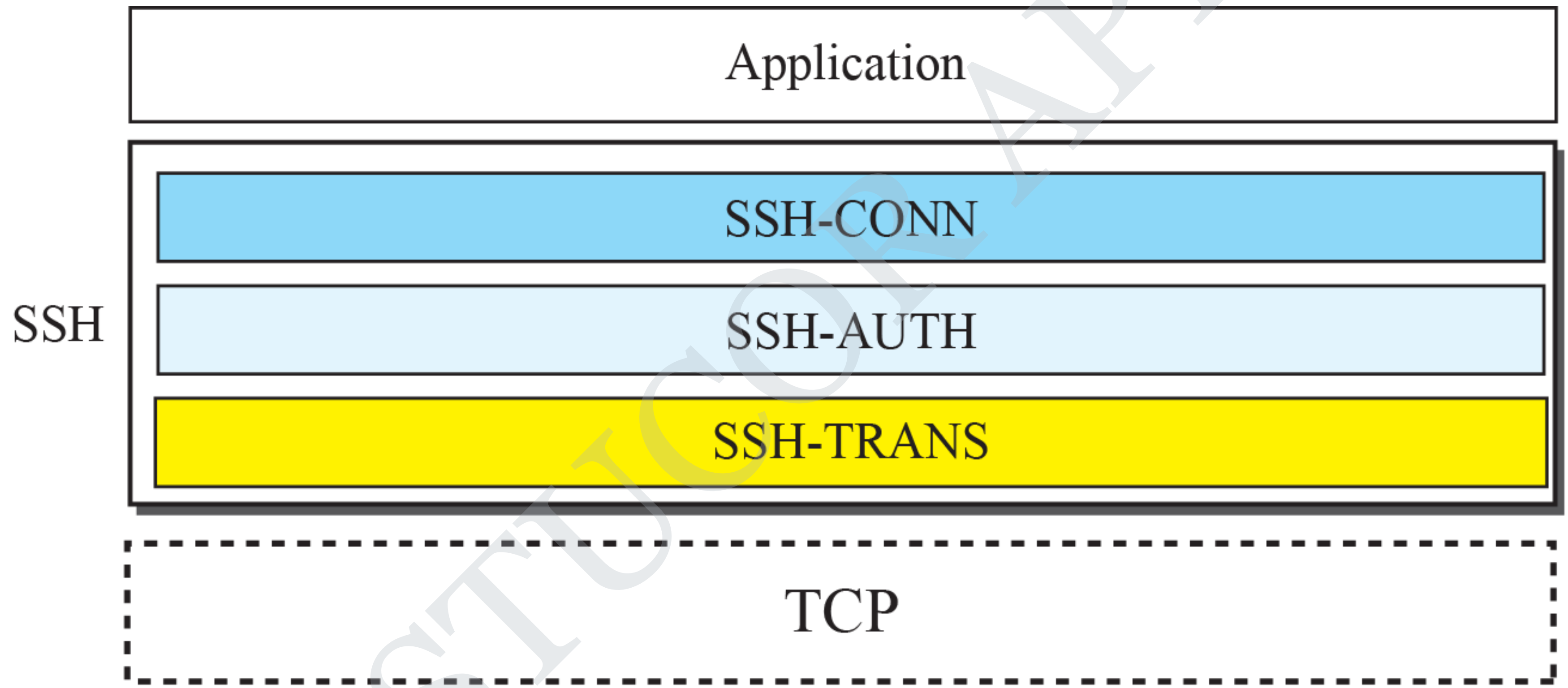


NVT character format

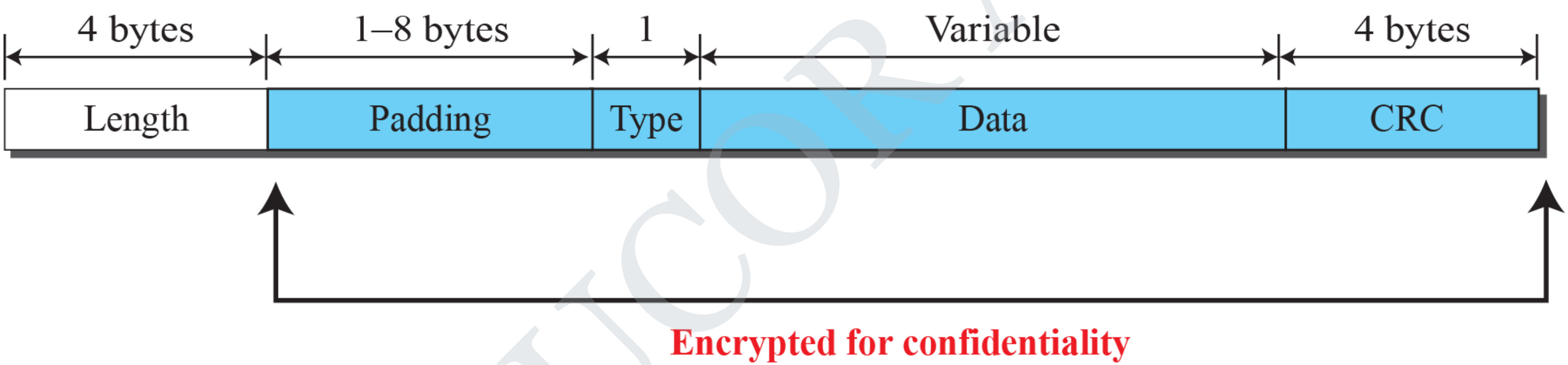
SECURE SHELL (SSH)

Although Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET. There are two versions of SSH. The first version, SSH-1, is now deprecated because of security flaws in it. In this section, we discuss only SSH-2.

Components of SSH



SSH Packet Format



DNS Components

There are 3 components:

- Name Space:

  Specifications for a structured name space and data associated with the names

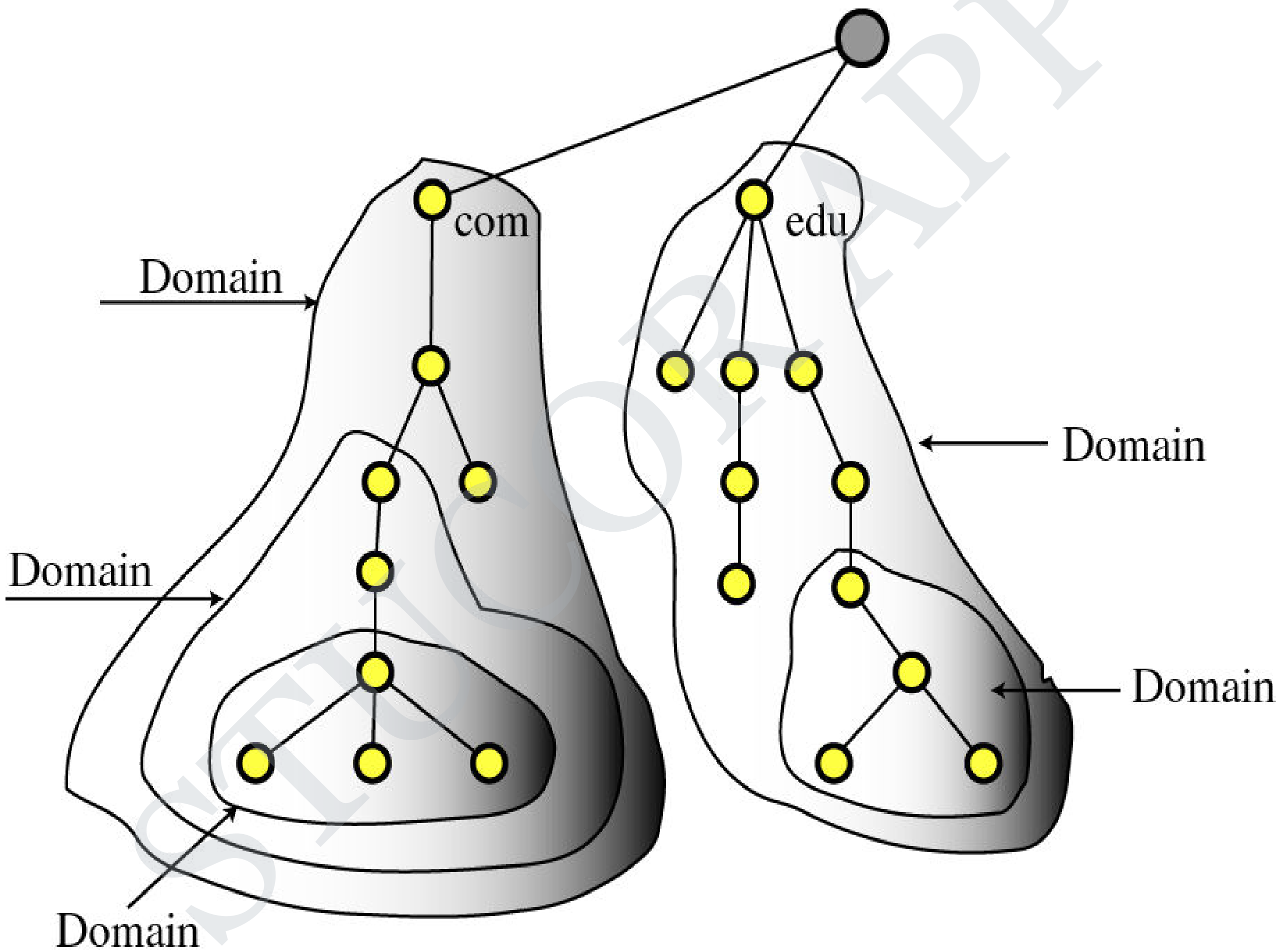
- Resolvers:

  Client programs that extract information from Name Servers.

- Name Servers:

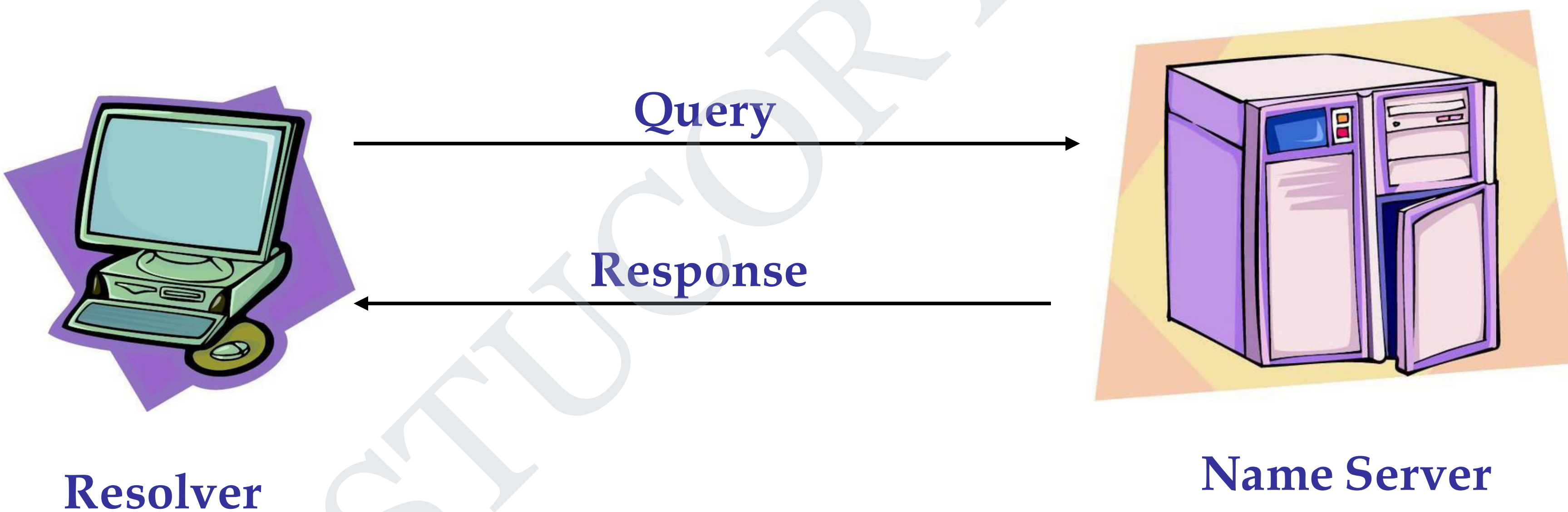
  Server programs which hold information about the structure and the names.

Name Space

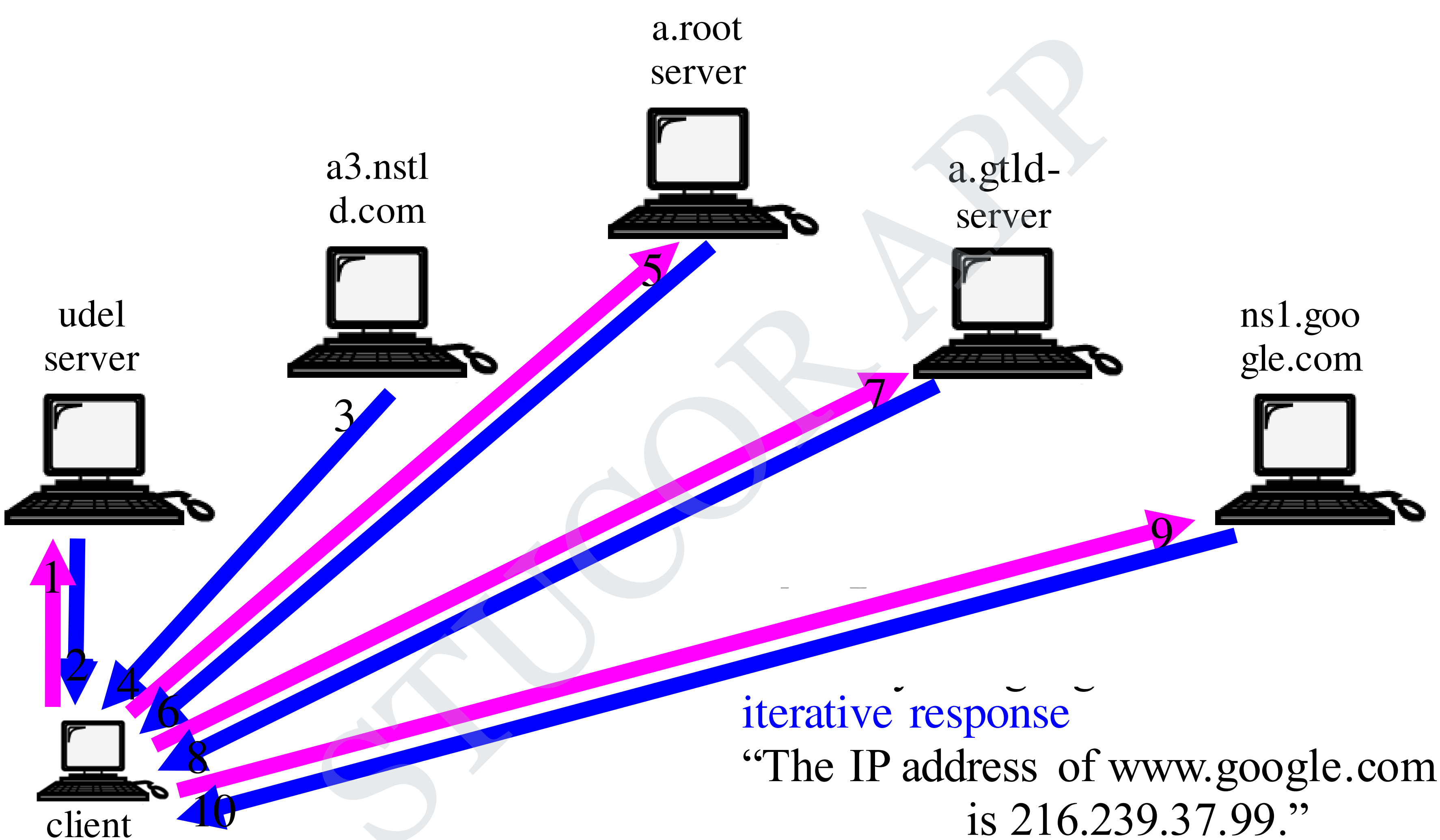


Resolvers

A Resolver maps a name to an address and vice versa.



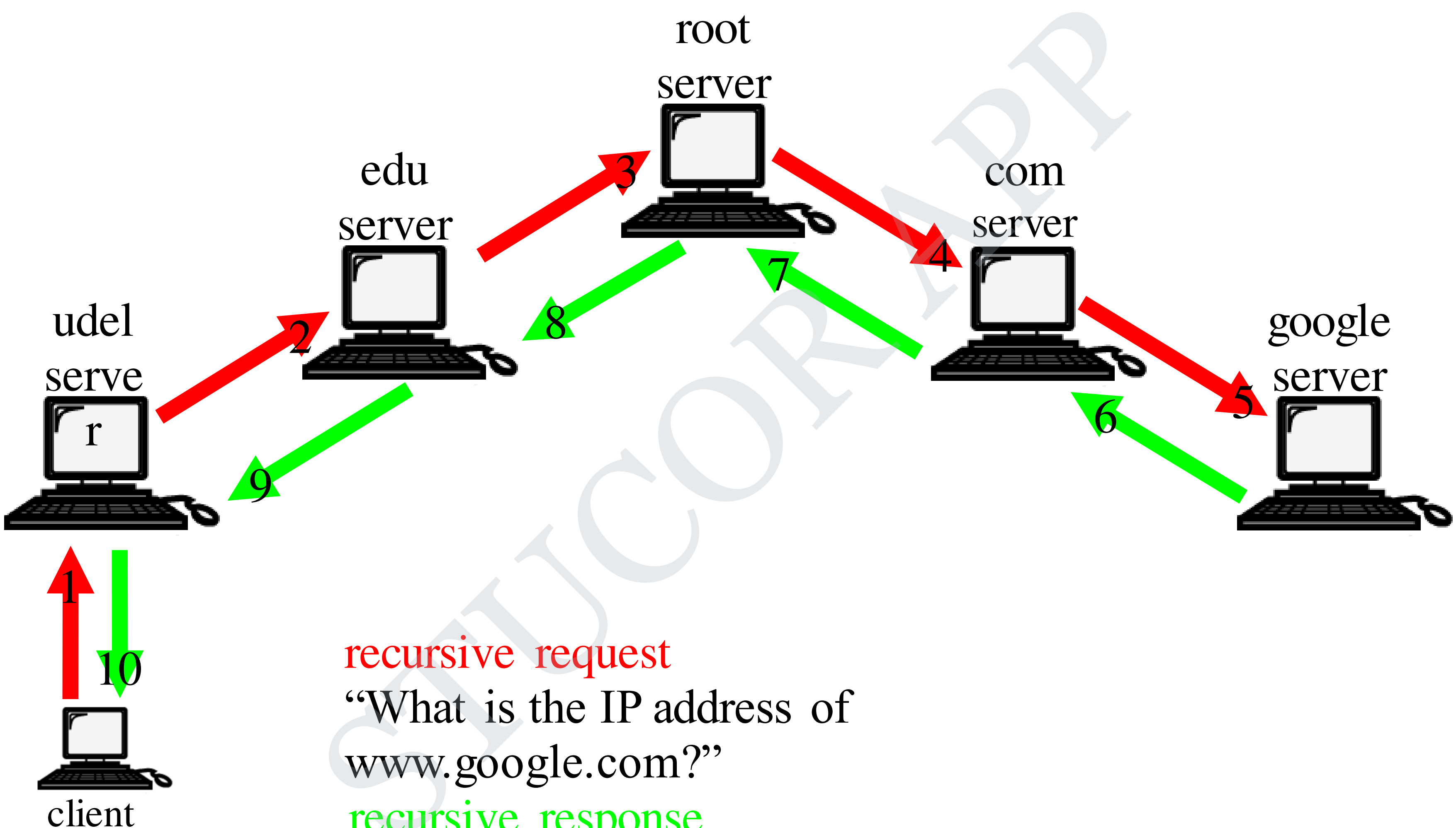
Iterative Resolution



iterative request

"What is the IP address of

Recursive Resolution



recursive request

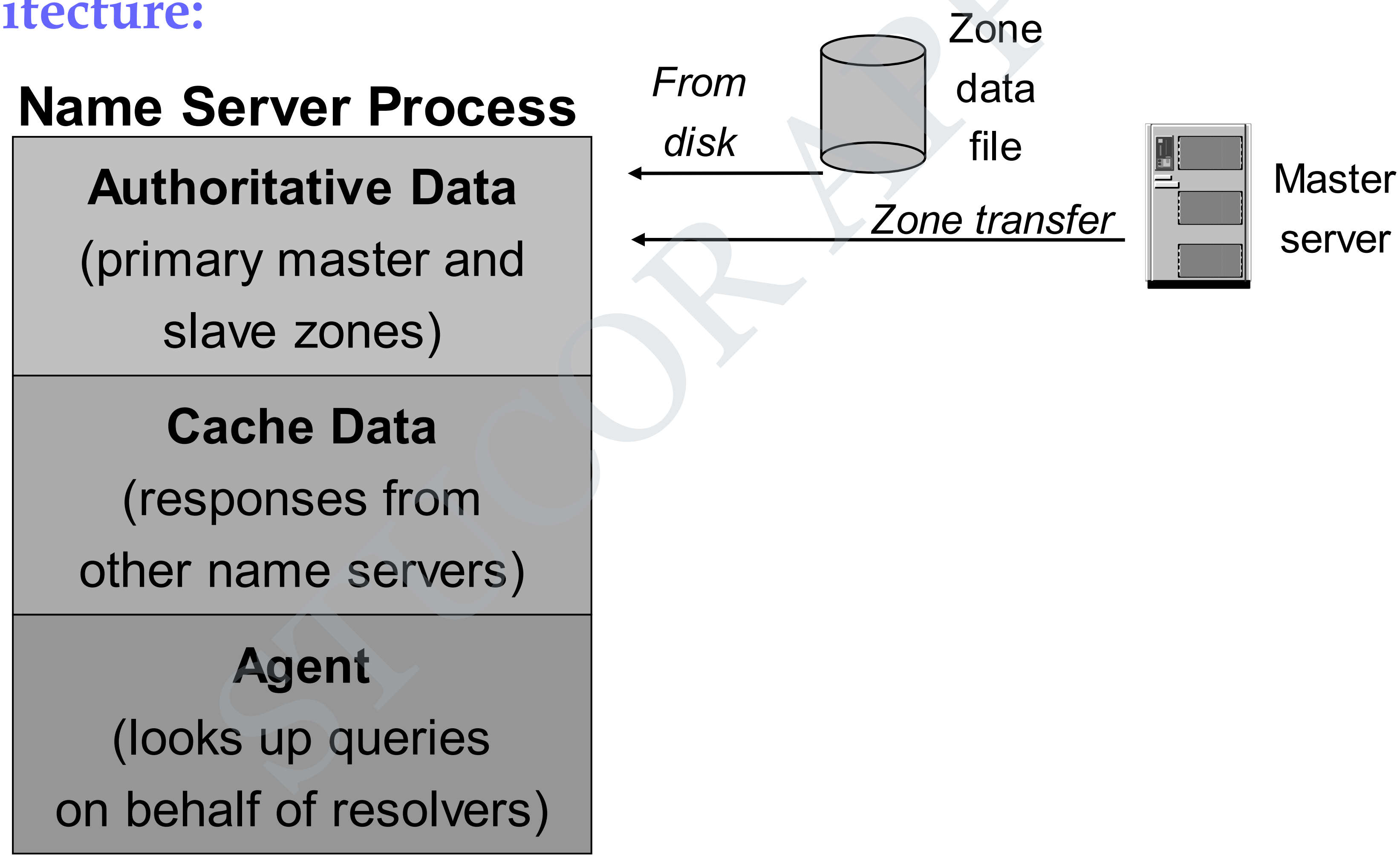
"What is the IP address of www.google.com?"

recursive response

"The IP address of www.google.com is 216.239.37.99."

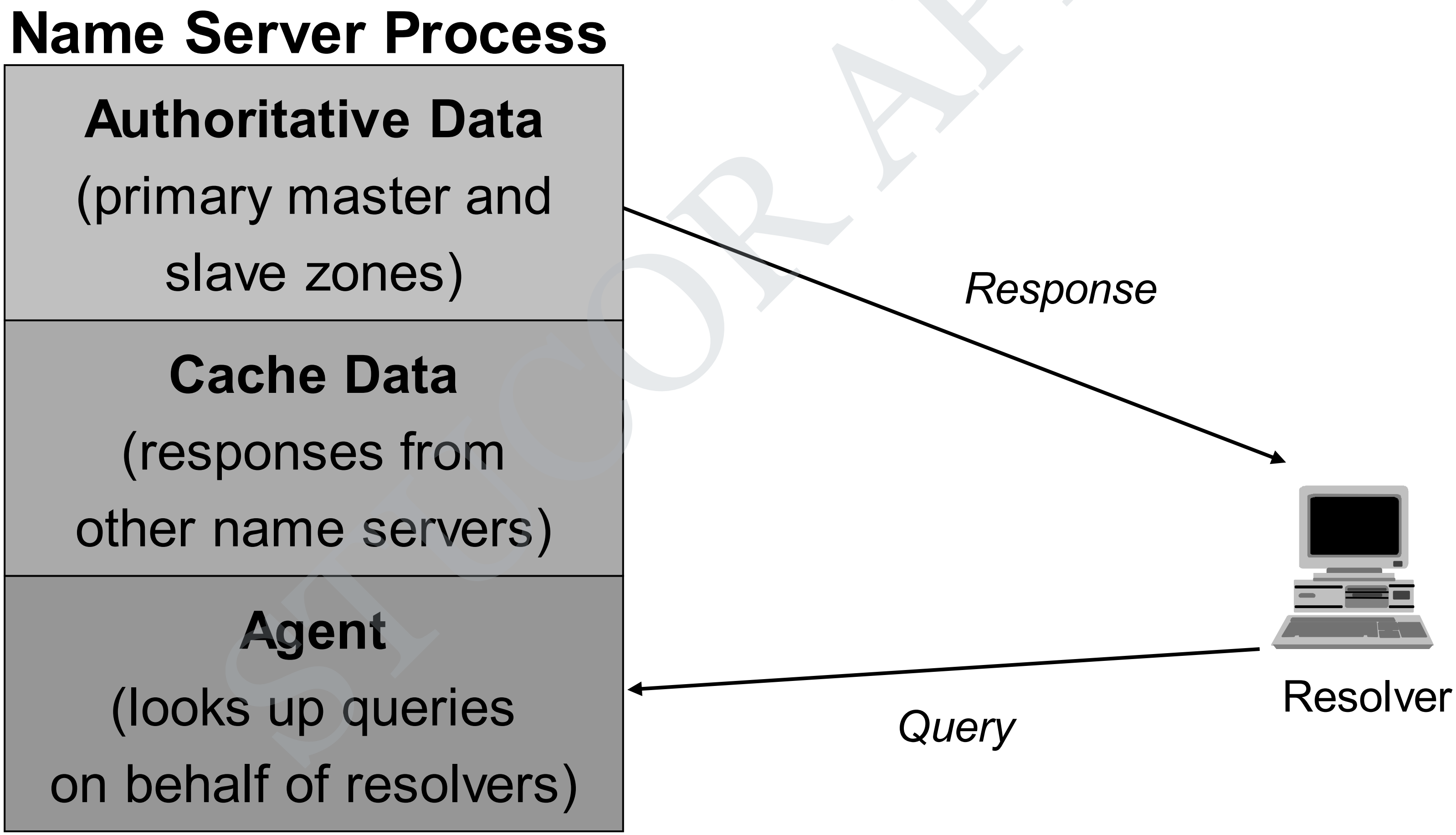
Name Server

Architecture:



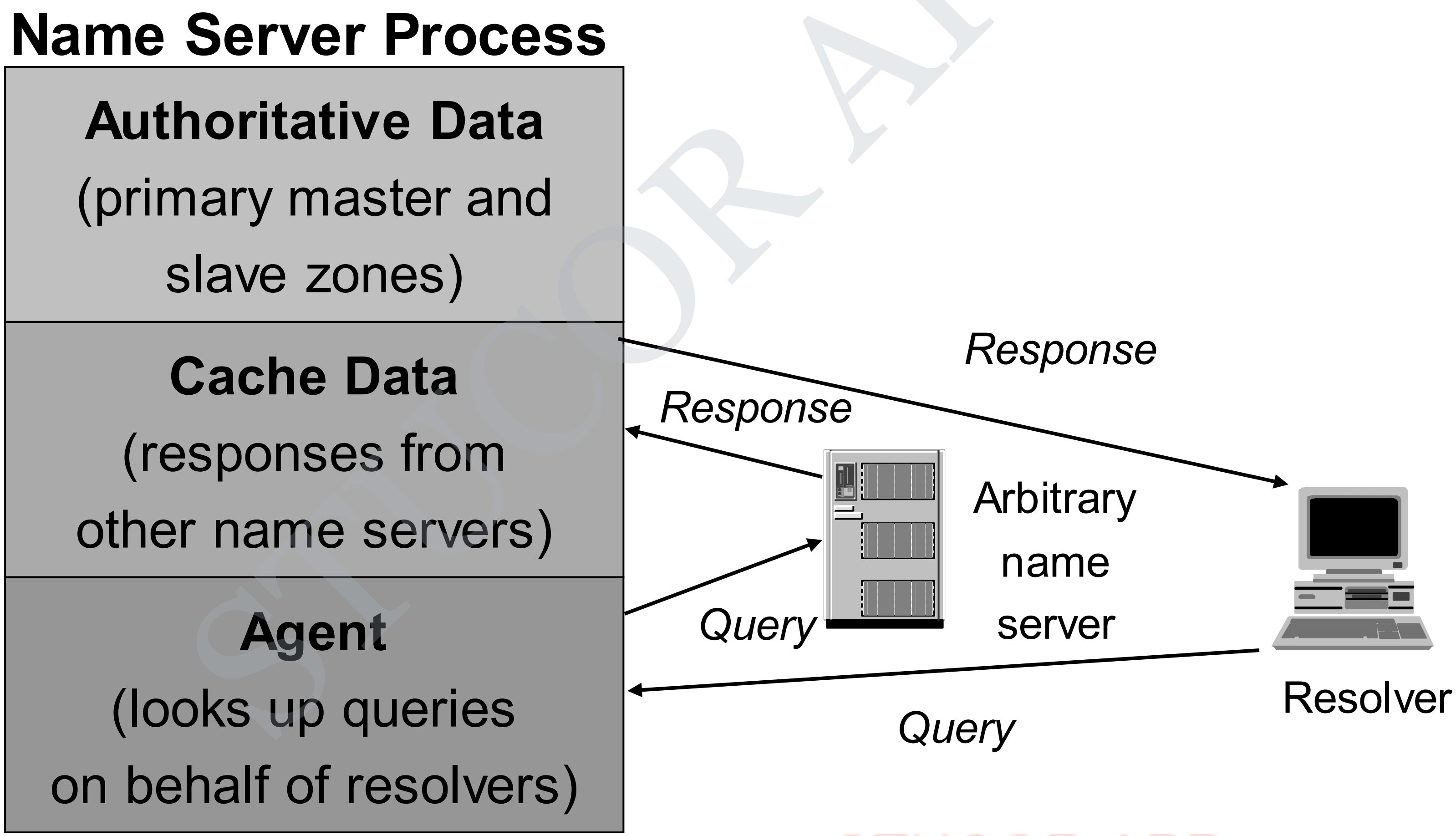
Name Server (cont'd)

Authoritative Data:



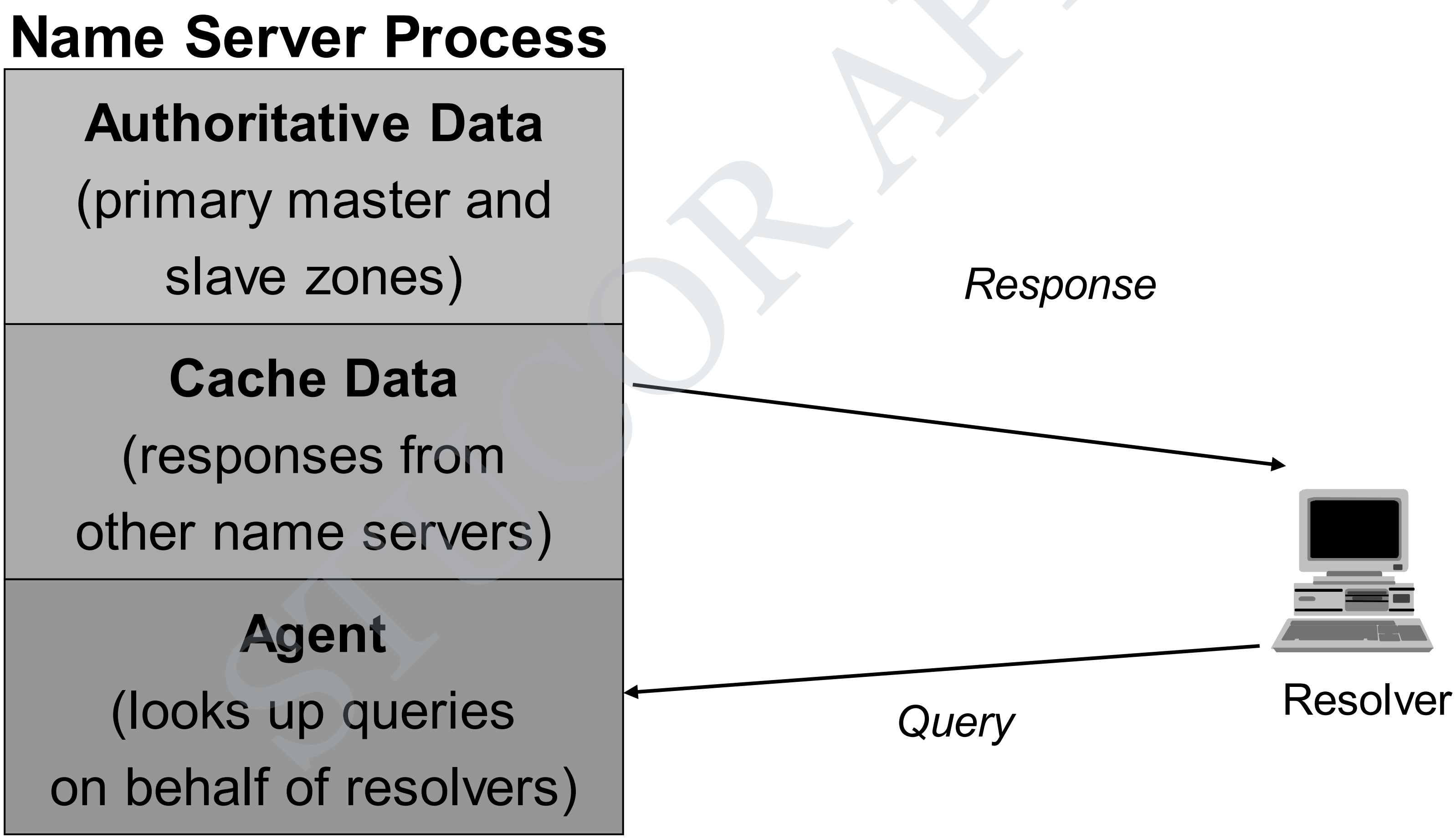
Name Server (cont'd)

Using Other Name Servers:

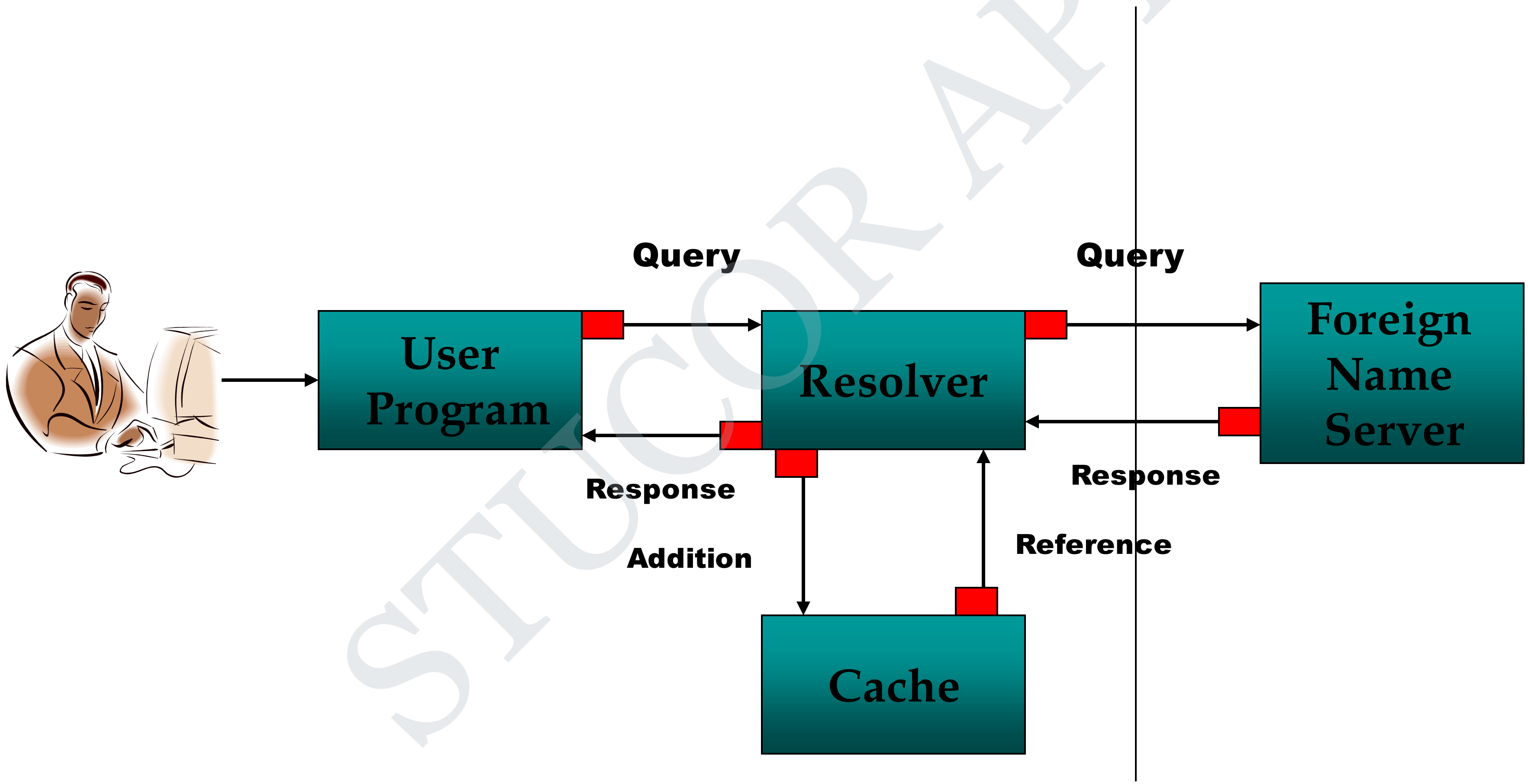


Name Server (cont'd)

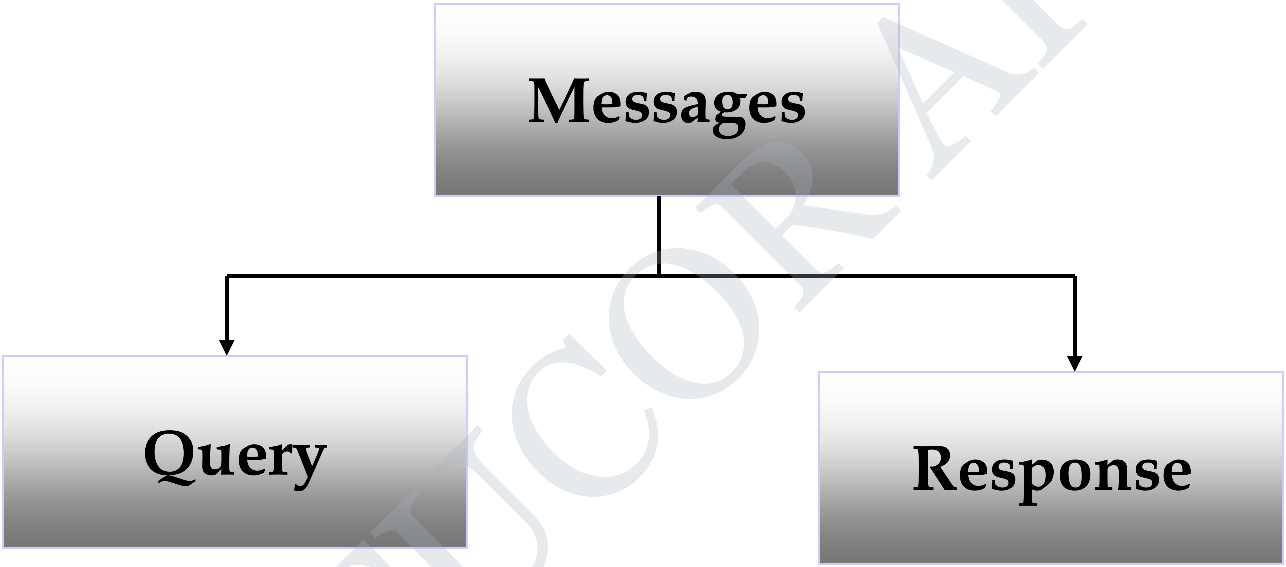
Cached Data :



Block Diagram



DNS Messages



What is Network Management?

Basic tasks that fall under this category are:

- Configuration Management
  - Keeping track of device settings and how they function
- Fault Management
  - Dealing with problems and emergencies in the network (router stops routing, server loses power, etc.)
- Performance Management
  - How smoothly is the network running?
  - Can it handle the workload it currently has?

SNMP Versions

- Two major versions SNMPv1, SNMPv2
- SNMPv1 is the recommended standard
- SNMPv2 has become split into:
  - SNMPv2u - SNMPv2 with user-based security
  - SNMPv2* - SNMPv2 with user-based security and additional features
  - SNMPv2c - SNMPv2 without security

What is SNMP?

- SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices.
- Comprised of agents and managers

•Agent - process running on each managed node collecting information about the device it is running on.

•Manager - process running on a management workstation that requests information about devices on the network.

Advantages of using SNMP

- Standardized
- universally supported
- extendible
- portable
- allows distributed management access
- lightweight protocol

Client Pull & Server Push

- SNMP is a "client pull" model

  The management system (client) "pulls" data from the agent (server).

- SNMP is a "server push" model

  The agent (server) "pushes" out a trap message to a (client) management system

The Three Parts of SNMP

SNMP network management is based on three parts:

- SNMP Protocol
  - Defines format of messages exchanged by management systems and agents.
  - Specifies the Get, GetNext, Set, and Trap operations
- Structure of Management Information (SMI)
  - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
- Management Information Base (MIB)
  - A map of the hierarchical order of all managed objects and how they are accessed