qwertyuiopasdfghjklzxcvbnmqwerty uiopasdfghj

klzxcv nmqw rtyuio

nmqwertyuiopasdfghjkl ertyuiopasdfghjklzxcvbnm pasdfghjklzxcvbnmqwert jklzxcvbnmqwertyuiopas

b

E-Content

ComputerNetwork(5thSem.)

Revti Raman, Lect.ECE

zxcvb qwe yuiop

asdfgh dfghj

klzxcvbnmqwertyuiopasdfghjklzxcvb nmqwertyuiopasdfghjklzxcvbnmqwe rtyuiopasdfghjklzxcvbnmqwertyuiop asdfghjklzxcvbnmqwertyuiopasdfghj klzxcvbnmqwertyuiopasdfghjklzxcvb nmqwertyuiopasdfghjklzxcvbnmqwe rtyuiopasdfghjklzxcvbnmqwertyuiop asdfghjklzxcvbnmqwertyuiopasdfghj klzxcvbnmqwertyuiopasdfghjklzxcvb nmrtyuiopasdfghjklzxcvbnmqwertyu iopasdfghjklzxcvbnmqwertyuiopasdf ghjklzxcvbnmqwertyuiopasdfghjklzx

cvbnmqwertyuiopasdfghjklzxcvbnmq

**UNITI-INTRODUCTIONANDPHYSICALLAYER**

**Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer : Performance – Transmission Media – Switching – Circuit Switched Networks – Packet Switching**

## INTRODUCTIONTONETWORKS

* A network isasetofdevices(oftenreferred toasnodes)connectedby communication links.
* Anodecanbeacomputer,printer,oranyotherdevicecapableofsendingor receiving data generated by other nodes on the network.
* When we communicate, we are sharing information. This sharing can be local or remote.

### CHARACTERISTICSOFANETWORK

Theeffectivenessofanetworkdependsonthreecharacteristics.

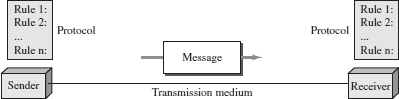
1. ***Delivery***:Thesystemmustdeliverdatatothecorrectdestination.
2. ***Accuracy***:Thesystemmustdeliverdataaccurately.
3. ***Timeliness***:Thesystemmustdeliverdatainatimely manner.

### CRITERIANECESSARYFORANEFFECTIVEANDEFFICIENTNETWORK

Anetworkmustbeabletomeetacertainnumberofcriteria.Themost importantof these are performance, reliability, and security.

|  |  |  |
| --- | --- | --- |
| ***Factors that affect the Performance of a network:*** | ***Factors that affect the Reliabilityof a network:*** | ***Factors that affect the Security of a network:*** |
| 1. Numberofusers 2. Typeoftransmission medium 3. Capabilities of the connectedhardware | 1. Efficiencyofsoftware. 2. Frequencyoffailure 3. Recovery time of a networkafterafailure | 1. Protecting data from unauthorizedaccessand viruses. |

### COMPONENTSINVOLVEDINANETWORKPROCESS

****

Thefivecomponentsare:

* 1. **Message** - It is the information to be communicated. Popular formsof information include text, pictures, audio, video etc.
  2. **Sender** - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.
  3. **Receiver** - It is the device which receives the data messages. It can bea computer, workstation, telephone handset etc.
  4. **Transmission Medium** - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radiowaves etc.
  5. **Protocol** - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

KEYELEMENTSOFPROTOCOL

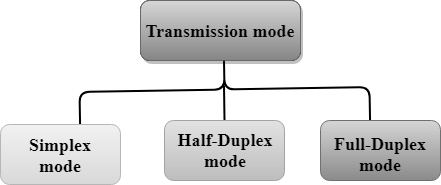
* + - ***Syntax***: Refers to the structure or format of the data, meaning the order in which they are presented.
    - ***Semantics***:Referstothemeaningofeachsectionofbits.
    - ***Timing***:Referstotwocharacteristics.(1).Whendatashouldbesentand(2).How fast they can be sent.

### TRANSMISSIONMODES

* Thewayinwhichdataistransmittedfromonedevicetoanotherdeviceisknown as **transmission mode**.
* Thetransmissionmodeisalsoknownasthecommunicationmode.
* Each communication channel has a direction associated with it, andtransmission mediaprovidethedirection. Therefore,thetransmissionmodeisalsoknownasa directional mode.
* Thetransmissionmodeisdefinedinthephysicallayer.

TypesofTransmissionmode

TheTransmissionmodeisdividedintothreecategories:

* SimplexMode
* Half-duplexMode
* Full-duplexmode(DuplexMode)

SIMPLEXMODE

* In Simplex mode,thecommunicationisunidirectional, i.e.,thedataflowinone direction.
* Adevicecanonlysendthedatabutcannotreceiveitoritcanreceivethedatabut cannot send the data.
* Thistransmissionmodeisnotverypopularasmainlycommunicationsrequirethe two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
* Theradiostationisasimplexchannelasittransmitsthesignaltothelistenersbut never allows them to transmit back.
* **KeyboardandMonitor**aretheexamplesofthesimplex modeasakeyboardcan only accept the data from the user and monitor can only be used to display the data on the screen.
* Themainadvantageofthesimplex modeisthatthefullcapacityofthe communication channel can be utilized during transmission.



AdvantageofSimplexmode:

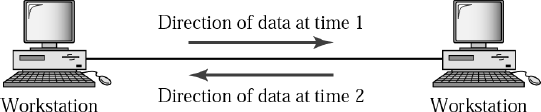
* In simplex mode, the station can utilize the entire bandwidth of the communicationchannel,sothatmoredatacanbetransmittedatatime.

DisadvantageofSimplexmode:

* Communicationisunidirectional,soithasnointer-communicationbetween devices.

HALF-DUPLEXMODE

* InaHalf-duplexchannel,directioncanbereversed,i.e.,thestationcantransmit and receive the data as well.
* Messagesflowinboththedirections,butnotatthesametime.
* Theentirebandwidthofthecommunicationchannelisutilizedinonedirectionat a time.
* Inhalf-duplex mode,itispossibletoperformtheerrordetection,andifanyerror occurs, then the receiver requests the sender to retransmit the data.
* A**Walkie-talkie**isanexampleoftheHalf-duplexmode.
* In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.



AdvantageofHalf-duplexmode:

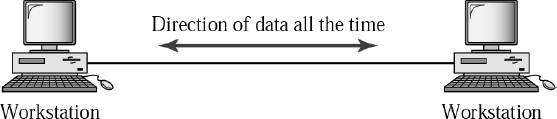
* Inhalf-duplex mode,boththedevicescansend andreceivethedataandalsocan utilize the entire bandwidth of the communication channel during the transmission of data.

DisadvantageofHalf-Duplexmode:

* Inhalf-duplex mode,whenonedeviceis sendingthedata,thenanotherhasto wait, this causes the delay in sending the data at the right time.

FULL-DUPLEXMODE

* InFullduplex mode,thecommunicationisbi-directional,i.e.,thedataflowin both the directions.
* Boththestationscansendandreceivethemessagesimultaneously.
* Full-duplexmodehastwosimplexchannels.Onechannelhastrafficmovingin onedirection, and anotherchannelhastrafficflowingintheoppositedirection.
* TheFull-duplexmodeisthefastestmodeofcommunicationbetweendevices.
* The most common example of the full-duplex mode is a T**elephone network**. Whentwopeoplearecommunicatingwitheachotherbyatelephoneline,both can talk and listen at the same time.



AdvantageofFull-duplexmode:

* Boththestationscansendandreceivethedataatthesametime.

DisadvantageofFull-duplexmode:

* Ifthereisnodedicatedpathexistsbetweenthe devices,thenthecapacityofthe communication channel is divided into two parts.

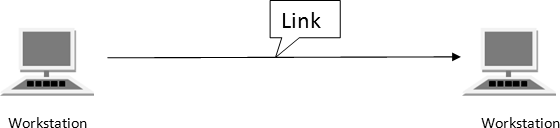
**COMPARISON-SIMPLEX,HALF-DUPLEXANDFULL-DUPLEXMODE**

|  |  |  |  |
| --- | --- | --- | --- |
| **BASIS FOR COMPARISON** | **SIMPLEX MODE** | **HALF-DUPLEX MODE** | **FULL-DUPLEX MODE** |
| Direction of communication | Communicationis unidirectional. | Communicationis bidirectional, but one at a time. | Communication is bidirectional. |
| Send/Receive | A device can only send the data but cannotreceiveitor it can only receive thedatabutcannot send it. | Both the devices can send and receive the data, butoneatatime. | Boththedevices can send and receive the data simultaneously. |
| Example | Radio,Keyboard, and monitor. | Walkie-Talkie | Telephone network. |

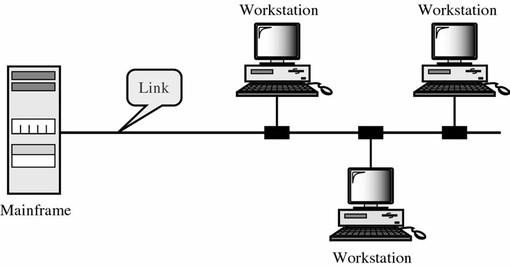
### LINECONFIGURATION/LINECONNECTIVITY

Line configuration refers to the way two or more communication devices attach to a link.Alinkisacommunicationspathwaythat transfersdatafromonedevicetoanother. There are two possible line configurations:

1. ***Point to Point* (PPP):** Provides a dedicated Communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.



1. ***MultiPoint* :** It is also called ***Multidrop*** configuration.In this connection two ormore devices share a single link.There are two kinds of Multipoint Connections.
   * **Spatial Sharing**: If several devices can share the link simultaneously, it is called Spatially shared line configuration
   * **Temporal(Time)Sharing**:Ifusersmusttaketurnsusingthelink, then its called Temporally shared or Time Shared Line Configuration.

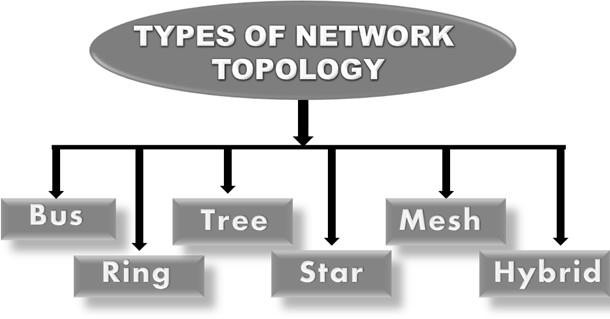


**NETWORKTOPOLOGY**

Two or more devices connect to a link. Two or more links form a topology.Topology is defined as

1. Thewayinwhichanetworkislaidoutphysically.
2. Thegeometricrepresentationoftherelationshipofallthelinksandnodesto one-another.

Thevarioustypesoftopologiesare:Bus,Ring,Tree,Star,MeshandHybrid.



BUSTOPOLOGY

* Bus topology is a network type in which every computer and network device isconnected to single cable.
* Thelongsinglecableactsasabackbonetolinkallthedevicesinanetwork.
* Whenithasexactlytwoendpoints,thenitiscalled**LinearBustopology.**
* Ittransmitsdataonlyinonedirection.



***DisadvantagesofBusTopology***

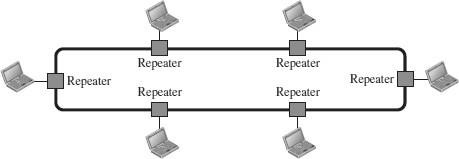
1. Cablesfailsthenwholenetworkfails.
2. Ifnetworktrafficisheavyornodesare more, the performance of the network decreases.
3. Cablehasalimitedlength.
4. Itisslowerthantheringtopology.

***AdvantagesofBusTopology***

1. Itiscosteffective.
2. Cablerequiredisleastcomparedto other network topology.
3. Usedinsmallnetworks.
4. Itiseasyto understand.
5. Easytoexpandjoiningtwocables together

RINGTOPOLOGY

* Inaringtopology,eachdevicehasadedicatedpoint-to-pointconnectionwith only the two devices on either side of it.
* A signal is passed along the ring in one direction, from device to device, until itreaches its destination.
* Eachdeviceintheringincorporatesarepeater.
* When a device receives a signal intended foranother device, its repeaterregenerates the bits and passes them along.



***DisadvantagesofRingTopology***

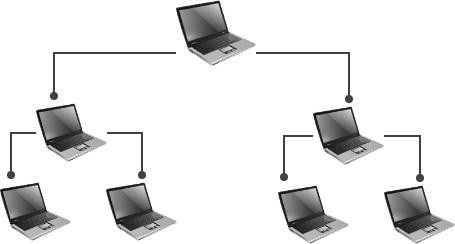
1. Troubleshootingisdifficultinring topology.
2. Addingordeletingthecomputers disturbs the network activity.
3. Failureofonecomputerdisturbsthe whole network

***AdvantagesofRingTopology***

1. Transmittingnetworkisnotaffectedby high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheaptoinstalland expand

TREETOPOLOGY

* + Ithasarootnodeandallothernodesareconnectedtoitforminga hierarchy.
  + Itisalsocalledhierarchicaltopology.
  + Itshouldatleasthavethreelevelstothehierarchy.
  + Treetopologyisidealifworkstationsarelocatedingroups.
  + TheyareusedinWideAreaNetwork.



***DisadvantagesofTreeTopology***

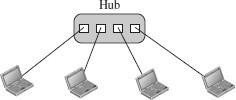
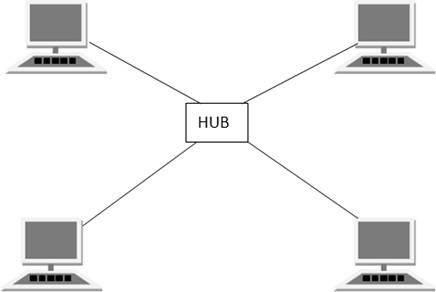
1. Heavilycabled.
2. Costly.
3. Ifmorenodesareaddedmaintenanceis difficult.
4. Centralhubfails,networkfails.

***AdvantagesofTreeTopology***

1. Extensionofbusandstar topologies.
2. Expansionofnodesispossibleandeasy.
3. Easilymanagedandmaintained.
4. Errordetectioniseasily done.

STARTOPOLOGY

* Inastartopology,eachdevicehasadedicatedpoint-to-pointlinkonlytoa central controller, usually called a hub.
* Thedevicesarenotdirectlylinkedtooneanother.
* Thecontrolleractsasanexchange.
* Ifonedevicewantstosenddatatoanother,itsendsthedatatothecontroller, which then relays the data to the other connected device.



***DisadvantagesofStarTopology***

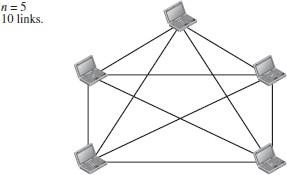
1. Costofinstallationishigh.
2. Expensivetouse.
3. Ifthehubfails,thenthewhole network is stopped.
4. Performanceisbasedonthehubthat is it depends on its capacity

***AdvantagesofStarTopology***

1. Fastperformancewithfewnodesand low network traffic.
2. Hubcanbeupgradedeasily.
3. Easytotroubleshoot.
4. Easytosetupandmodify.
5. Onlythatnodeisaffectedwhichhas failed, rest of the nodes can work smoothly

MESHTOPOLOGY

* Inameshtopology,everydevicehasadedicatedpoint-to-pointlinktoevery other device.
* Thetermdedicatedmeansthatthelinkcarriestrafficonlybetweenthetwodevices it connects.
* The number of physical links in a fully connected mesh network with *n* nodes is given by *n* (*n* – 1) / 2.



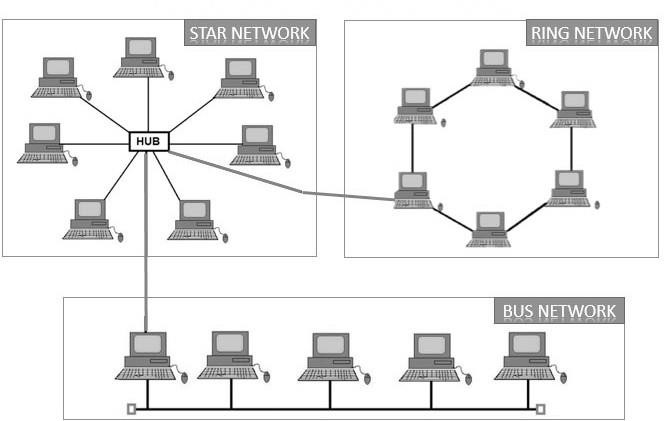
***DisadvantagesofMeshTopology***

1. Installationandconfigurationis difficult.
2. Cablingcostis more.
3. Bulkwiringisrequired.

***AdvantagesofMeshTopology***

1. Eachconnectioncancarryitsowndata load.
2. Itisrobust.
3. Faultisdiagnosedeasily.
4. Providessecurityandprivacy.

HYBRIDTOPOLOGY

* HybridTopologyisacombinationofoneormorebasictopologies.
* For example if one department in an office uses ring topology, the other departments uses star and bus topology, then connecting these topologies will result in Hybrid Topology.
* Hybrid Topology inherits the advantages and disadvantages of the topologies included.

***DisadvantagesofHybridTopology***

1. Complexindesign.
2. Costly

***AdvantagesofHybridTopology***

1. ReliableasErrordetectingandtrouble shooting is easy.
2. Effective.
3. Scalableassizecanbeincreasedeasily.
4. Flexible.

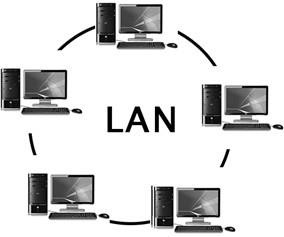
## NETWORKTYPES

* A computer networkis a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
* Acomputernetworkcanbecategorizedbytheirsize.
* Acomputernetworkismainlyofthreetypes:

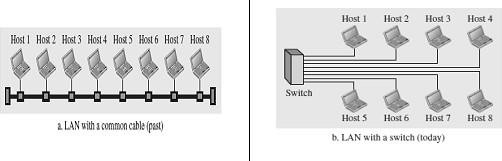
1. LocalAreaNetwork(LAN)
2. WideAreaNetwork(WAN)
3. MetropolitanAreaNetwork(MAN)

LOCALAREANETWORK(LAN)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.



* Itislesscostlyasitisbuiltwithinexpensivehardwaresuchashubs,network adapters, and ethernet cables.
* ThedataistransferredatanextremelyfasterrateinLocalAreaNetwork.
* LANcanbeconnectedusingacommoncableoraSwitch.



***DisadvantagesofLAN***

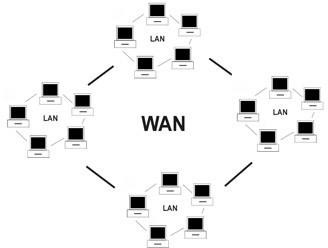
* HighSetupCost
* PrivacyViolations
* DataSecurityThreat
* LANMaintenanceJob
* CoversLimitedArea

***Advantagesof LAN***

* ResourceSharing
* SoftwareApplicationsSharing.
* EasyandCheap Communication
* CentralizedData.
* DataSecurity
* InternetSharing

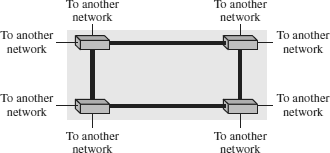
WIDEAREANETWORK(WAN)

* A WideArea Network is a network that extends over a largegeographical areasuch as states or countries.
* AWideAreaNetworkisquitebiggernetworkthantheLAN.



* AWide Area Networkis not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
* TheinternetisoneofthebiggestWANintheworld.
* A Wide Area Network is widely used in the field of Business, government, andeducation.
* WANcanbeeitherapoint-to-pointWANorSwitchedWAN.

***Point-to-pointWAN SwitchedWAN***

******

***DisadvantagesofWideAreaNetwork****:*

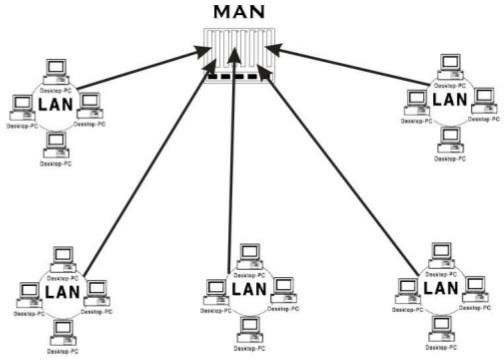
* Securityissue
* NeedsFirewall&antivirussoftware
* HighSetupcost
* Troubleshootingproblems

***AdvantagesofWideAreaNetwork*:**

* LargeGeographicalarea
* Centralizeddata
* Exchangemessages
* Sharingofsoftwareandresources
* Highbandwidth

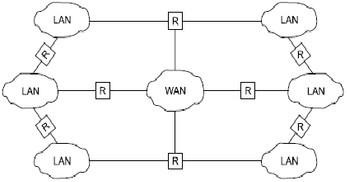
METROPOLITANAREANETWORK(MAN)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Itgenerallycoverstownsandcities(50km)
* In MAN, variousLANs are connected to each other through a telephoneexchange line.
* CommunicationmediumusedforMANareopticalfibers,cablesetc.
* Ithasahigherrangethan LocalArea Network(LAN).Itisadequatefordistributed computing applications.



INTERNETWORK

* AninternetworkisdefinedastwoormorecomputernetworkLANsorWAN.
* AnInternetwork can be formed by joining two or more individual networksbymeans of various devices such as routers, gateways and bridges.
* An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.

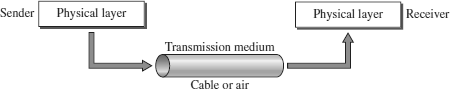


**TypesofInternetwork**

|  |  |
| --- | --- |
| ***Extranet*** | ***Intranet*** |
| An extranet is used for informationsharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it musthave one connection to the **external network**. | An intranet belongs to an organization whichisonlyaccessiblebythe **organization's employee** or members. The main aimof the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences. |

## TRANSMISSIONMEDIA

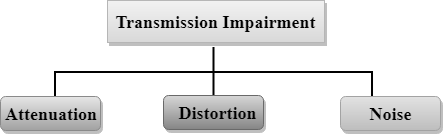
* Transmission mediaisacommunicationchannelthatcarriestheinformationfrom the sender to the receiver.
* Dataistransmittedthroughtheelectromagneticsignals.
* Themainfunctionalityofthetransmissionmediaistocarrytheinformationin the form of bits (Either as Electrical signals or Light pulses).
* Itisaphysicalpathbetweentransmitterandreceiverindatacommunication.
* The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
* Transmissionmediaisoftwotypes:GuidedMedia(Wired)andUnGuided Media (wireless).
* In guided (wired) media, medium characteristics are more important whereas, in unguided (wireless) media, signal characteristics are more important.
* Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
* ThetransmissionmediaisavailableinthelowestlayeroftheOSIreference model, i.e., Physical layer.



FACTORSFORDESIGNINGTHETRANSMISSIONMEDIA

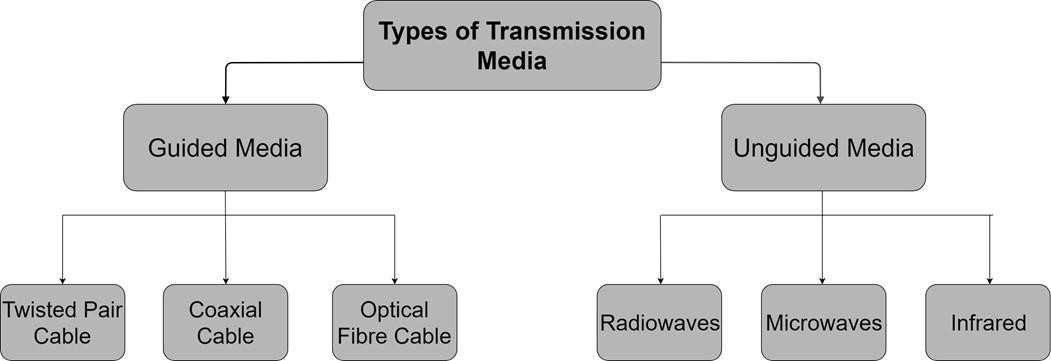
* **Bandwidth:** Allthefactorsareremainingconstant,thegreaterthebandwidthof a medium, the higher the data transmission rate of a signal.
* **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signalswill get destroyed due to transmission impairment.
* **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

CAUSESOFTRANSMISSIONIMPAIRMENT

****

* **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
* **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
* **Noise:**Whendataistravelledoveratransmissionmedium,someunwantedsignal is added to it which creates the noise.

**TYPES/CLASSESOFTRANSMISSIONMEDIA**

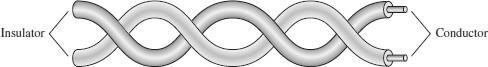
****

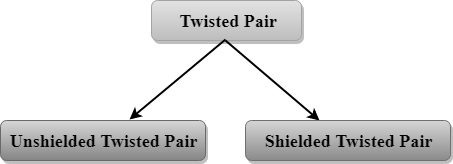
### GUIDEDMEDIA

* Itisdefinedasthephysicalmediumthroughwhichthesignalsaretransmitted.
* ItisalsoknownasBoundedmedia.
* TypesofGuidedmedia:TwistedPairCable,CoaxialCable,FibreOpticCable

TWISTEDPAIRCABLE

* Twistedpairisaphysicalmediamadeupofapairofcablestwistedwitheach other.
* Atwistedpaircableischeapascomparedtoothertransmissionmedia.
* Installationofthetwistedpaircableiseasy,anditisalightweight cable.
* Thefrequencyrangefortwistedpaircableisfrom0to3.5KHz.
* A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

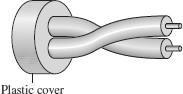




**UnshieldedTwistedPair**

Anunshieldedtwistedpairiswidelyusedin telecommunication. Followingarethecategoriesoftheunshieldedtwistedpaircable:

* **Category1:**Suportslow-speeddata.
* **Category2:**Itcansupportupto4Mbps.
* **Category3:**Itcansupportupto16Mbps.
* **Category4:**Itcansupportupto20Mbps.
* **Category5:**Itcansupportupto200Mbps.



Advantages:

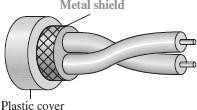
* Itischeap.
* Installationoftheunshieldedtwistedpairiseasy.
* Itcanbeusedforhigh-speed LAN.

Disadvantage:

* Thiscablecanonlybeusedforshorterdistancesbecauseofattenuation.

**ShieldedTwistedPair**

Ashieldedtwistedpairisacablethatcontainsthemeshsurroundingthewirethatallows the higher transmission rate.



Advantages:

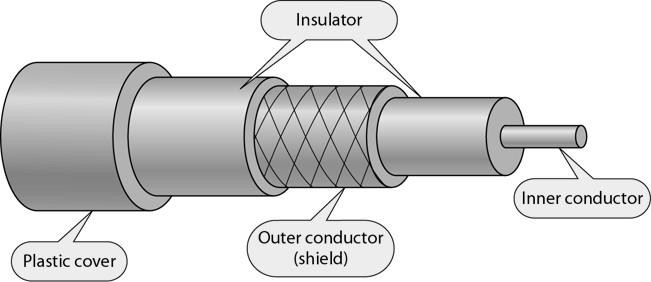
* Thecostoftheshieldedtwistedpaircableisnotveryhighandnotverylow.
* InstallationofSTPiseasy.
* Ithashighercapacityascomparedtounshieldedtwistedpaircable.
* Ithasahigherattenuation.
* Itisshieldedthatprovidesthehigherdatatransmissionrate.

Disadvantages:

* ItismoreexpensiveascomparedtoUTPandcoaxialcable.
* Ithasahigherattenuationrate.

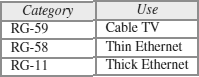
COAXIALCABLE

* Coaxial cable(Coax) is a very commonly used transmission media, for example, TV wire is usually a coaxial cable.
* Thenameofthecableiscoaxialasitcontainstwoconductorsparalleltoeach other.
* IthasahigherfrequencyascomparedtoTwistedpaircable.
* Theinnerconductorofthecoaxialcableismadeupofcopper,andtheouter conductor is made up of copper mesh.
* Themiddlecoreismadeupofnon-conductivecoverthatseparatestheinner conductor from the outer conductor.
* The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).
* CommonapplicationsofcoaxialcableareCableTVnetworksand traditional Ethernet LANs.



CoaxialCableStandards

* Coaxialcablesarecategorizedbytheir**RadioGovernment(RG)**ratings.
* Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing.
* EachcabledefinedbyanRGratingisadaptedforaspecializedfunction.



TypesofCoaxialcable:

1. ***Basebandtransmission*:**Itisdefinedastheprocessoftransmittingasingle

signalathighspeed.

1. ***Broadbandtransmission*:**Itisdefinedastheprocessoftransmittingmultiple

signalssimultaneously.

Advantages:

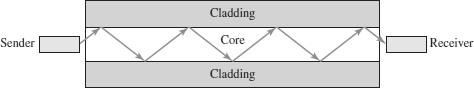
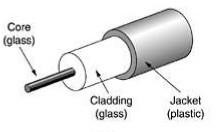
* + Thedatacanbetransmittedathighspeed.
  + Ithasbettershieldingascomparedtotwistedpaircable.
  + Itprovideshigherbandwidth.

Disadvantages:

* + Itismoreexpensiveascomparedtotwistedpaircable.
  + Ifanyfaultoccursinthecablecausesthefailure intheentirenetwork.

FIBREOPTICCABLE

* + Fibreopticcableisacablethatuseselectricalsignalsforcommunication.
  + Fibre optic is a cablethat holds the optical fibres coated in plastic thatare used to send the data by pulses of light.
  + Theplasticcoatingprotectstheopticalfibresfromheat,cold,electromagnetic interference from other types of wiring.
  + Fibreopticsprovidefasterdatatransmissionthancopperwires.



BasicelementsofFibreopticcable:

* + ***Core*:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of thecore, the more light will be transmitted into the fibre.
  + ***Cladding*:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
  + ***Jacket*:**The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Advantages:

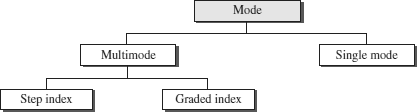
* + GreaterBandwidth
  + Lesssignalattenuation
  + Immunitytoelectromagneticinterference
  + Resistancetocorrosivematerials
  + Lightweight
  + Greaterimmunitytotapping

Disadvantages:

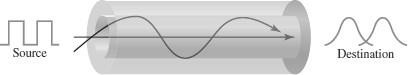
* + RequiresExpertiseforInstallationandmaintenance
  + Unidirectionallightpropagation.
  + HigherCost.

#### PropagationModesofFibre Optics

* Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics.
* Multimodecanbeimplementedintwoforms:step-indexorgraded-index.



###### MultimodePropagation

* Multimodeissonamedbecause multiplebeamsfromalightsource movethrough the core in different paths.
* Howthesebeamsmovewithinthecabledependsonthestructureofthecore.



* The multimode graded-index fiber**,** decreasesthisdistortionofthesignal through the cable.
* Theword*index*herereferstotheindex of refraction.
* Theindexofrefractionisrelatedto density.
* Agradedindexfiber,therefore,isone with varying densities.
* Densityishighestatthecenterofthe core and decreases gradually to its lowest at the edge.

**MultimodeGraded-indexfiber**

**MultimodeStep-indexfiber**

Inmultimodestep-indexfiber**,**thedensity of the core remains constant from the center to the edges.

A beam of light moves through this constantdensityinastraightlineuntilit reaches the interface of the core andthe cladding.

* At the interface, there is an abrupt change duetoalowerdensity;thisalterstheangle of the beam’s motion.

The term *step-index* refers to the suddenness of this change, which contributestothedistortionofthesignal as it passes through the fiber.

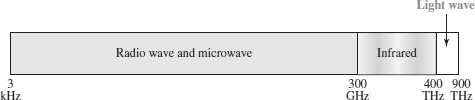
###### Single-ModePropagation

****

* Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
* The single-mode fiber itself is manufactured with a much smaller diameter than thatofmultimodefiber, andwithsubstantiallylowerdensity(indexofrefraction).
* The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.
* In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination “together” and can be recombined with little distortion to the signal.

### UNGUIDEDMEDIA

* Anunguided transmission transmits the electromagnetic waves without usingany physical medium. Therefore it is also known as **wireless transmission**.
* Inunguidedmedia,airisthemediathroughwhichtheelectromagneticenergy can flow easily.

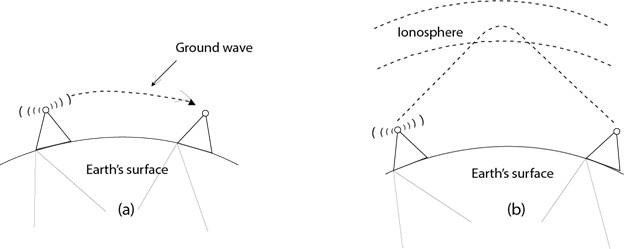


* Unguidedtransmissionisbroadlyclassifiedintothreecategories:

RadioWaves,Microwaves,Infrared

RADIOWAVES

* + Radio waves are the electromagnetic waves that are transmitted in all thedirections of free space.
  + Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
  + Therangeinfrequenciesofradiowavesisfrom3Khzto1Khz.
  + Inthecaseofradio waves, thesendingandreceivingantennaare notaligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
  + Anexampleoftheradiowaveis**FMradio**.



ApplicationsofRadiowaves:

* + ARadiowaveisusefulformulticastingwhenthereisonesenderandmany receivers.
  + AnFMradio,television,cordlessphonesareexamplesofaradiowave.

AdvantagesofRadiowaves:

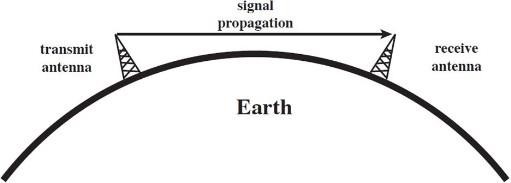
* + Radiotransmissionismainlyusedforwideareanetworksandmobilecellular phones.
  + Radiowavescoveralargearea,andtheycanpenetratethewalls.
  + Radiotransmissionprovidesahighertransmissionrate.

MICROWAVES

Microwavesareoftwotypes-Terrestrialmicrowave&Satellitemicrowave

**TerrestrialMicrowave**

* + Terrestrial Microwave transmission is a technology that transmits the focused beamofaradiosignalfromone ground-based microwavetransmissionantennato another.
  + Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
  + Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focused.
  + In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
  + It works on the line of sight transmission, i.e., the antennas mounted on thetowers are at the direct sight of each other.



CharacteristicsofTerrestrialMicrowave:

* + **Frequencyrange:**Thefrequencyrangeofterrestrialmicrowaveisfrom4-6GHz to 21-23 GHz.
  + **Bandwidth:**Itsupportsthebandwidthfrom1to10Mbps.
  + **Shortdistance:**Itisinexpensiveforshortdistance.
  + **Longdistance:** Itisexpensiveasitrequiresahighertowerforalongerdistance.
  + **Attenuation:**Attenuationmeanslossofsignal.Itisaffectedbyenvironmental conditions and antenna size.

AdvantagesofTerrestrialMicrowave:

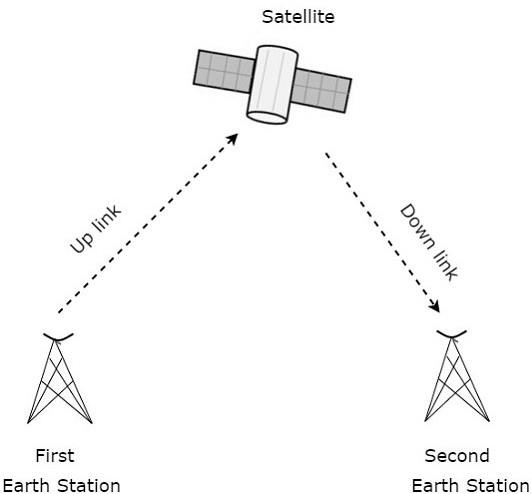
* + Microwavetransmissionischeaperthanusingcables.
  + It is free from land acquisition as it does not require any land for the installation of cables.
  + Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
  + Communicationoveroceanscanbeachievedbyusingmicrowavetransmission.

DisadvantagesofTerrestrialMicrowave:

* + Eavesdropping**.**
  + Outofphase signal
  + Susceptibletoweathercondition
  + Bandwidthlimited

**SatelliteMicrowave**

* + Asatelliteisaphysicalobjectthatrevolvesaroundtheearthataknownheight.
  + Satellitecommunicationismorereliablenowadaysasitoffersmoreflexibility than cable and fibre optic systems.
  + We can communicate with any point on the globe by using satellite communication.
  + Thesatelliteacceptsthesignalthatistransmittedfromtheearthstation,andit amplifies the signal.The amplified signalis retransmitted to another earthstation.



AdvantagesofSatelliteMicrowave:

* + Thecoverageareaofasatellitemicrowaveismorethantheterrestrialmicrowave.
  + Thetransmissioncostofthesatelliteisindependentofthedistancefromthe centre of the coverage area.
  + Satellite communication is used in mobile and wireless communication applications.
  + Itiseasyto install.
  + It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

DisadvantagesofSatelliteMicrowave:

* + Satellitedesigninganddevelopmentrequiresmoretimeandhighercost.
  + TheSatelliteneedstobemonitoredandcontrolledonregularperiodssothatit remains in orbit.
  + The life ofthe satelliteis about12-15 years. Due to thisreason, another launch of the satellite has to be planned before it becomes non-functional.

INFRAREDWAVES

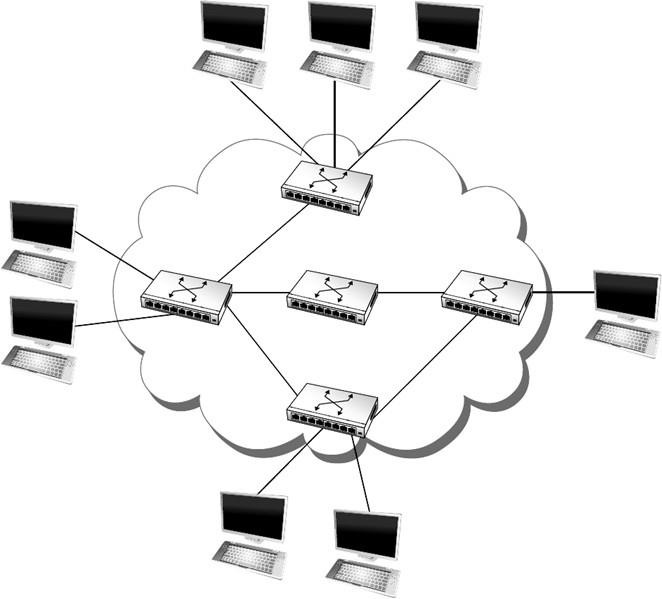
* + An infrared transmission is a wireless technology used for communication over short ranges.
  + Thefrequencyoftheinfraredintherangefrom300GHzto400 THz.
  + It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone and devices that resides in the same closed area.

CharacteristicsofInfrared:

* + Itsupportshighbandwidth,andhencethedataratewillbeveryhigh.
  + Infraredwavescannotpenetrate thewalls. Therefore, theinfraredcommunication in one room cannot be interrupted by the nearby rooms.
  + Aninfraredcommunicationprovidesbettersecuritywithminimuminterference.
  + Infraredcommunicationisunreliableoutsidethebuilding becausethesunrays will interfere with the infrared waves.

**SWITCHING**

* + Thetechniqueoftransferringtheinformationfromonecomputernetworkto another network is known as **switching**.
  + Switchinginacomputernetworkisachievedbyusingswitches.
  + Aswitchisasmallhardwaredevicewhichisusedtojoinmultiplecomputers together with one local area network (LAN).
  + Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
  + SwitchesareusedtoforwardthepacketsbasedonMACaddresses.
  + ASwitch is used totransfer thedata onlytothedevice that has been addressed.It verifies the destination address to route the packet appropriately.
  + Itisoperatedinfullduplexmode.
  + Itdoesnotbroadcastthemessageasitworkswithlimitedbandwidth.



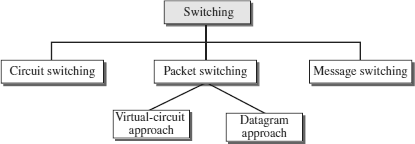
AdvantagesofSwitching:

* + Switchincreasesthebandwidthofthenetwork.
  + ItreducestheworkloadonindividualPCsasitsendstheinformationtoonlythat device which has been addressed.
  + Itincreasestheoverallperformanceofthenetworkbyreducingthetrafficonthe network.
  + Therewillbelessframecollisionasswitchcreatesthecollisiondomainforeach connection.

DisadvantagesofSwitching:

* + ASwitchismoreexpensivethannetworkbridges.
  + ASwitchcannotdeterminethenetworkconnectivityissueseasily.
  + Properdesigningandconfigurationoftheswitcharerequiredtohandlemulticast packets.

**TypesofSwitchingTechniques**

****

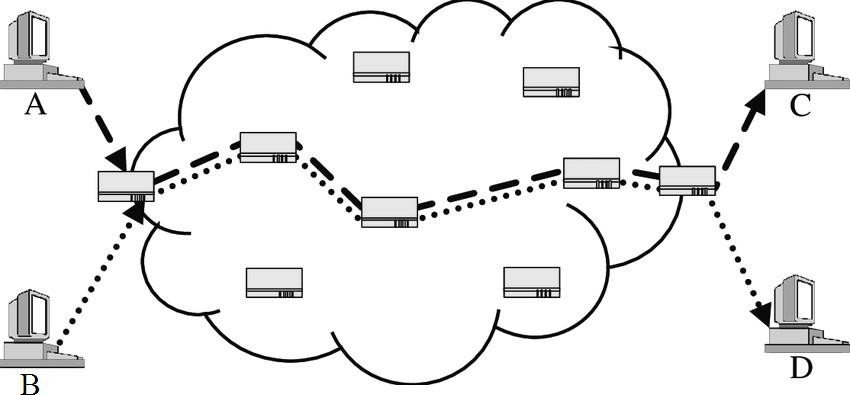
### CIRCUITSWITCHING

* + Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
  + In the Circuit Switching Technique, once the connection is established then thededicated path will remain to exist until the connection is terminated.
  + Circuitswitchinginanetworkoperatesinasimilarwayasthetelephoneworks.
  + Acompleteend-to-endpathmustexistbeforethecommunicationtakesplace.
  + In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
  + Circuit switching is used in public telephone network. It is used for voice transmission.
  + Fixeddatacanbetransferredatatimeincircuitswitchingtechnology.

PhasesinCircuitSwitching

Communicationthroughcircuitswitchinghas3phases:

1. ***Connection Setup / Establishment*** - In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
2. ***Data transfer*** - Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.
3. ***Connection teardown / Termination*** - When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.



Advantages

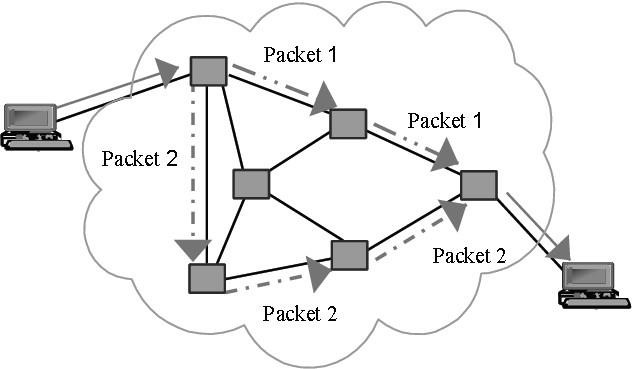
* + Itissuitableforlong continuoustransmission,sinceacontinuoustransmission route is established, that remains throughout the conversation.
  + Thededicatedpathensuresasteadydatarateofcommunication.
  + Nointermediatedelaysarefoundoncethecircuitisestablished.So,theyare suitable for real time communication of both voice and data transmission.

Disadvantages

* + Circuitswitchingestablishesadedicatedconnectionbetweentheendparties.This dedicated connection cannot be used for transmitting any other data, even if the data load is very low.
  + Bandwidthrequirementishighevenincasesoflowdatavolume.
  + There is underutilization of system resources. Once resources are allocated to a particular connection, they cannot be used for other connections.
  + Timerequiredtoestablishconnectionmaybehigh.
  + It is more expensive than other switching techniques as a dedicated path is required for each connection.

### PACKETSWITCHING

* Thepacketswitchingisaswitchingtechnique inwhichthemessageissentinone go, but it is divided into smaller pieces, and they are sent individually.
* The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
* Everypacketcontainssomeinformationinitsheaderssuchassourceaddress, destination address and sequence number.
* Packetswilltravelacrossthenetwork,takingtheshortestpathaspossible.
* Allthepacketsarereassembledatthereceivingendincorrectorder.
* If any packet is missing or corrupted, then the message will be sent to resend the message.
* If the correct order of the packets is reached, then the acknowledgment message will be sent.



AdvantagesofPacketSwitching:

* **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost- effective technique.
* **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
* **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

DisadvantagesofPacketSwitching:

* Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
* Theprotocolsusedinapacketswitchingtechniqueareverycomplexandrequires high implementation cost.
* If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

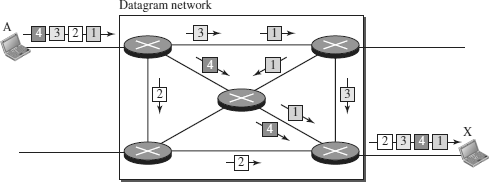
APPROACHESOFPACKETSWITCHING

TherearetwoapproachestoPacketSwitching:

* DatagramPacketswitching
* VirtualCircuitSwitching

#### DatagramPacketswitching

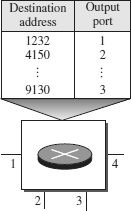
* Itisapacketswitchingtechnologyinwhichpacketisknownasadatagram,is considered as an independent entity.
* Each packet contains the information about the destination and switch uses thisinformation to forward the packet to the correct destination.
* Thepacketsarereassembledatthereceivingendincorrectorder.
* InDatagramPacketSwitchingtechnique,thepathisnotfixed.
* Intermediatenodestaketheroutingdecisionstoforwardthepackets.
* DatagramPacketSwitchingisalsoknownasconnectionlessswitching.
* Therearenosetuporteardownphases.
* Eachpacketistreatedthesamebyaswitchregardlessofitssourceordestination.



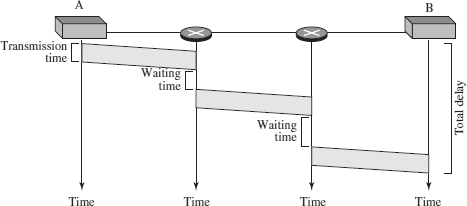
In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination.

RoutingTable

In this type ofnetwork, each switch(orpacket switch) hasa routingtable whichis based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the correspondingforwardingoutput ports are recorded in the tables.



Delayinadatagramnetwork

******

* + Thepackettravelsthroughtwoswitches.
  + There are three transmission times (3*T*),three propagation delays (slopes 3t of the lines), and two waiting times (*w*1 + *w*2).
  + Weignoretheprocessingtimeineachswitch.

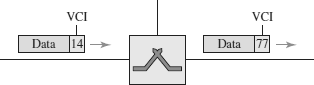
**Totaldelay=3*T+* 3t+*w*1+*w*2**

#### VirtualCircuitSwitching

* VirtualCircuitSwitchingisalsoknownasconnection-orientedswitching.
* In the case of Virtual circuit switching, a virtual connection is established before the messages are sent.
* Call request and call accept packets are used to establish the connection between sender and receiver.
* Inthiscase,thepathisfixedforthedurationofalogicalconnection.

VirtualCircuitIdentifier(VCI)

A virtual circuit identifier (VCI) that uniquely identifies the connection at this switch. A VCI, unlike a global address, is a small number that has only switch scope; it is used bya frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.



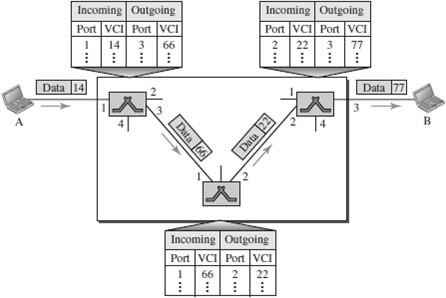
VirtualCircuitTable

EveryVirtualCircuit(VC)maintainsatablecalledVirtualCircuittable. One entry in the VC table on a single switch contains the following :

* + AnincominginterfaceonwhichpacketsforthisVCarriveattheswitch
  + AnoutgoinginterfaceinwhichpacketsforthisVCleavetheswitch
  + AoutgoingVCIthatwillbeusedforoutgoingpackets

Example:

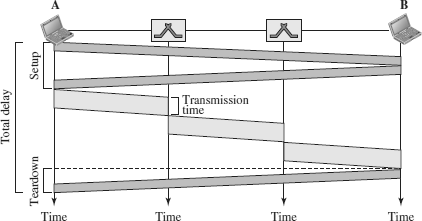
SourceAsendsaframetoSourceBthroughSwitch1,Switch2andSwitch3.



TypesofVirtualCircuits

TherearetwobroadclassesofVirtualCircuits. They are

1. PVC–PermanentVirtualCircuit
   * NetworkAdministratorwillconfigurethestate
   * Thevirtualcircuitispermanent(PVC)
2. SVC–SwitchedVirtualCircuit
   * A hostcansendmessagesintothenetworktocausethestatetobe established. This is referred as signaling.
   * AhostmaysetupanddeletesuchaVCdynamicallywithoutthe involvement of a network administrator

DelayinVirtual-CircuitNetworks

* Thepacketistravelingthroughtwoswitches(routers).
* There are three transmission times (3*T* ), three propagation times (3t),data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction).

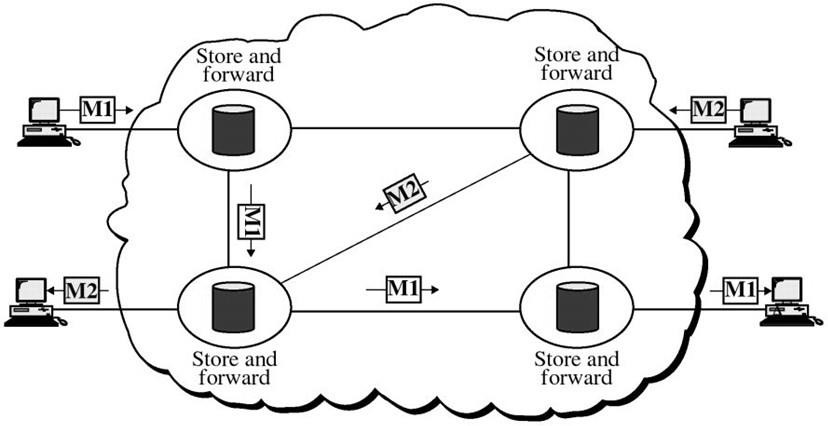
**Totaldelay=3*T+*3t+Setupdelay+Teardowndelay**

### COMPARISON–CIRCUITSWITCHINGANDPACKETSWITCHING

|  |  |  |
| --- | --- | --- |
| **CIRCUIT** | **PACKETSWITCHING** | |
| **SWITCHING** | **VirtualCircuitSwitching** | **DatagramSwitching** |
| Connectionoriented | Connectionoriented | Connectionless |
| Ensuresinorder delivery | Ensuresinorderdelivery | Packetsmaybedeliveredout of order |
| Noreorderingisrequired | Noreorderingisrequired | Reorderingisrequired |
| Adedicatedpathexists for data transfer | Adedicatedpathexistsfor data transfer | Nodedicatedpathexistsfor data transfer |
| Allthepacketstakethe same path | Allthepacketstakethe same path | Allthepacketsmaynottake the same path |
| Resourcesareallocated before data transfer | Resourcesareallocatedon demand using 1st packet | Noresourcesareallocated |
| Streamoriented | Packetoriented | Packetoriented |
| Fixedbandwidth | DynamicBandwidth | Dynamicbandwidth |
| Reliable | Reliable | Unreliable |
| No overheads | Lessoverheads | Higheroverheads |
| Implementedatphysical layer | Implementedatdatalink layer | Implementedatnetwork layer |
| Inefficientintermsof resource utilization | Providesbetterefficiency than circuit switched  systems | Providesbetterefficiency than message switched  systems |
| Example-Telephone systems | Examples-X.25,Frame relay | Example-Internet |

**MESSAGESWITCHING**

* Message Switching is a switching technique in which a message is transferred asa complete unit and routed through intermediate nodes at which it is stored and forwarded.
* In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
* The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
* Message switches are programmed in such a way so that they can provide the most efficient routes.
* Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
* Messageswitchingtreatseachmessageasanindependententity.



**PROTOCOLLAYERING**

* In networking, a protocol **defines the rules** that both the sender and receiver and all intermediate devices need to follow to be able **to communicate effectively**.
* Aprotocolprovidesacommunicationservicethattheprocessusetoexchange messages.
* Whencommunicationissimple,wemayneedonlyonesimpleprotocol.
* When the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**
* Protocol layering is that it allows us to separate the services from the implementation.
* A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer.
* Anymodificationinonelayerwillnotaffecttheotherlayers.

**BasicElementsofLayeredArchitecture**

* **Service:**Itisasetofactionsthatalayerprovidestothehigherlayer.
* **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
* **Interface:** It is a way through which the message is transferred from one layer to another layer.

**FeaturesofProtocolLayering**

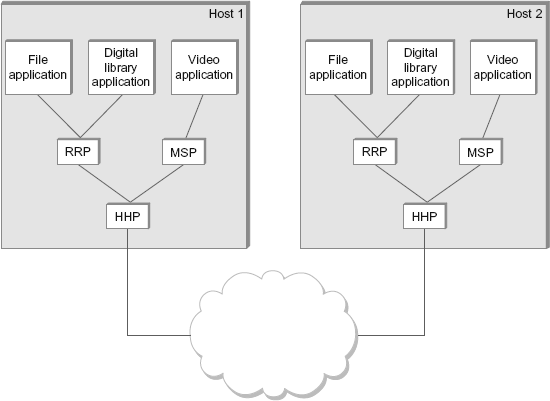
1. **Itdecomposestheproblemofbuildinganetwork**intomoremanageable components.
2. Itprovidesamoremodulardesign.

**PrinciplesofProtocolLayering**

1. The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
2. The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

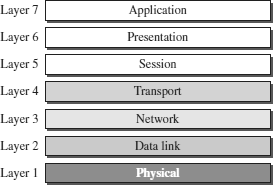
**ProtocolGraph**

* + Thesetofprotocolsthatmakeupanetworksystemiscalleda**protocolgraph**.
  + The nodes of the graph correspond to protocols, and the edges represent a dependence relation.
  + For example, the Figure below illustrates a protocol graph consists of protocols ***RRP (Request/Reply Protocol)*** and ***MSP (Message Stream Protocol)*** implement two different types of process-to-process channels, and both depend on the ***HHP (Host-to- Host Protocol)*** which provides a host-to-host connectivity service

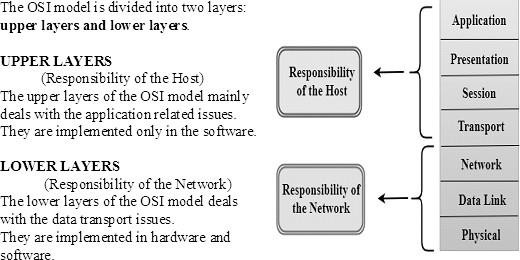


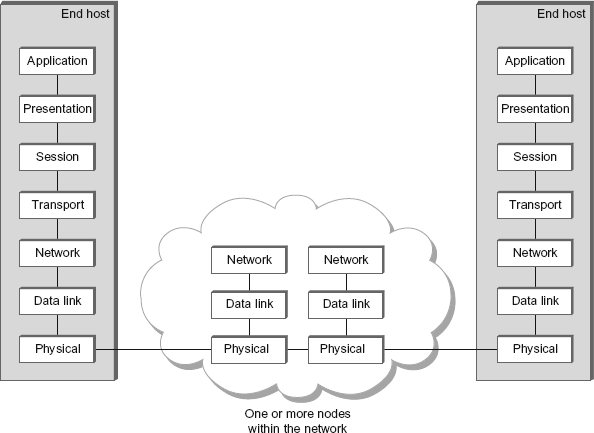
## OSIMODEL

* OSIstandsfor**OpenSystemInterconnection.**
* Itisareference modelthatdescribeshowinformationfromasoftwareapplication in one computer moves through a physical medium to the software application in another computer.
* OSI consists of seven layers, and each layer performs a particular network function.
* OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter- computer communications.
* OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
* Each layer is self-contained, so that task assigned to each layer can be performed independently.



**ORGANIZATIONOFTHEOSILAYERS**

****

****

### FUNCTIONSOFTHEOSILAYERS

1. PHYSICALLAYER

The physical layer coordinates the functions required to **transmit a bit stream over a physical medium.**

Thephysicallayerisconcernedwiththefollowingfunctions:

* + **Physical characteristics of interfaces and media -** The physical layer definesthe characteristics of the interface between the devices and the transmission medium.
  + **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
  + **Signals:**Itdeterminesthetypeofthesignalusedfortransmittingtheinformation.
  + **Data Rate or Transmission rate -** The number of bits sent each second –is also defined by the physical layer.
  + **Synchronization of bits -** The sender and receiver must be synchronized at thebit level. Their clocks must be synchronized.
  + **Line Configuration -** In a point-to-point configuration, two devicesare connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
  + **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.
  + **TransmissionMode-**Thephysicallayeralsodefinesthedirectionof transmission between two devices: simplex, half-duplex or full-duplex.

1. DATALINKLAYER

Itisresponsiblefor**transmittingframesfromonenodetothenextnode**. The other responsibilities of this layer are

* + **Framing-**Dividesthestreamofbitsreceivedintodataunitscalledframes.
  + **Physical addressing** – If frames are to be distributed to different systems on the network , data link layer adds a header to the frame to define the sender and receiver.
  + **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
  + **Error control**- Used for detectingand retransmittingdamaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
  + **Medium Access control** -Used to determine which device has control over the link at any given time.

1. NETWORK LAYER

Thislayerisresponsibleforthe**deliveryofpacketsfromsourcetodestination**.

Itdeterminesthebestpathtomovedatafromsourcetothedestinationbasedonthe network conditions, the priority of service, and other factors.

Theotherresponsibilitiesofthislayerare

* + **Logical addressing** - If a packet passes the network boundary, we need another addressing system for source and destination called logical address. This addressing is used to identify the device on the internet.
  + **Routing** – Routing is the major component of the network layer, andit determines the best optimal path out of the multiple paths from source to the destination.

1. TRANSPORTLAYER

It is responsible for **Process to Process** delivery. That is responsible for source-to- destination (end-to-end) delivery of the entire message, It also ensures whether the message arrives in order or not.

Theotherresponsibilitiesofthislayerare

* + **Port addressing / Service Point addressing** - The header includes an address called port address / service point address. This layer gets the entire message to the correct process on that computer.
  + **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
  + **Connectioncontrol**-Thiscaneitherbe**connectionlessorconnectionoriented.**
    - The connectionless treats each segment as an individual packet anddelivers to the destination.
    - The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
  + **Flowcontrol**- Thetransportlayeralsoresponsibleforflowcontrolbutitis performed end-to-end rather than across a single link.
  + **ErrorControl-**Errorcontrolisperformedend-to-endratherthanacrossthe single link..

1. SESSIONLAYER

Thislayer**establishes, managesandterminatesconnectionsbetweenapplications**. The other responsibilities of this layer are

* + **Dialog control** - Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
  + **Synchronization**- Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

1. PRESENTATIONLAYER

It is concerned with the **syntaxandsemantics ofinformationexchanged betweentwo systems.**

Theotherresponsibilitiesofthislayerare

* + **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
  + **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
  + **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

1. APPLICATIONLAYER

This layer **enables theuserto access thenetwork**.It handlesissues such as network transparency, resource allocation, etc. This allows the user to log on to remote user.

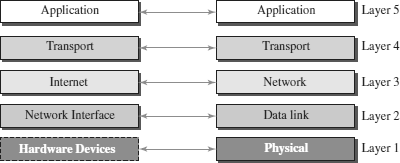
Theotherresponsibilitiesofthislayerare

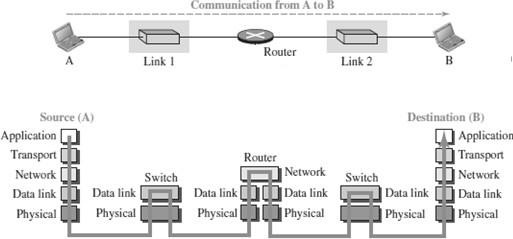
* + **FTAM (File Transfer, Access, Management)** - Allows user to access files in a remote host.
  + **Mailservices**-Providesemailforwardingand storage.
  + **Directory services** - Provides database sources to access information about various sources and objects.

### TCP/IPPROTOCOLSUITE

* TheTCP/IParchitectureisalsocalledasInternetarchitecture.
* ItisdevelopedbytheUSDefenseAdvanced ResearchProject Agency(**DARPA**) for its packet switched network (**ARPANET**).
* TCP/IPisaprotocolsuiteusedintheInternettoday.
* Itisa4-layermodel.ThelayersofTCP/IP are

1. **Applicationlayer**
2. **TransportLayer(TCP/UDP)**
3. **InternetLayer**
4. **NetworkInterfaceLayer**

****

****

APPLICATIONLAYER

* Anapplicationlayerincorporatesthefunctionof topthreeOSIlayers.An application layer is the topmost layer in the TCP/IP model.
* Itisresponsibleforhandlinghigh-levelprotocols,issuesofrepresentation.
* Thislayerallowstheusertointeractwiththeapplication.
* Whenoneapplicationlayerprotocolwantstocommunicatewithanother application layer, it forwards its data to the transport layer.
* Protocols such as FTP, HTTP, SMTP, POP3, etc running in the application layer provides service to other program running on top of application layer

TRANSPORTLAYER

* The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
* The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
  + **UDP** – UDP provides connectionless service and end-to-end delivery of transmission.Itisanunreliableprotocolasitdiscoverstheerrorsbutnot specify the error.
  + **TCP** – TCP provides a full transport layer services to applications. TCP is a reliable protocol as it detects the error and retransmits the damaged frames.

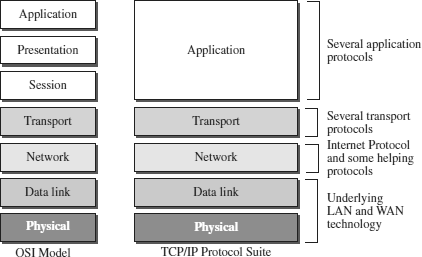
INTERNETLAYER

* TheinternetlayeristhesecondlayeroftheTCP/IP model.
* Aninternetlayerisalsoknownasthenetworklayer.
* The main responsibility of the internet layer is to send the packets from any network,andtheyarriveatthedestinationirrespectiveoftheroutetheytake.
* Internetlayerhandlethetransfer ofinformationacrossmultiplenetworksthrough router and gateway .
* IPprotocolisusedinthislayer,anditisthemostsignificantpartoftheentire TCP/IP suite.

NETWORKINTERFACELAYER

* ThenetworkinterfacelayeristhelowestlayeroftheTCP/IPmodel.
* This layer is the combination of the Physical layer and Data Linklayer defined in the OSI reference model.
* Itdefineshowthedatashouldbesentphysicallythroughthenetwork.
* This layer is mainly responsible for the transmission of the data between two devices on the same network.
* The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
* The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

## COMPARISON-OSIMODELANDTCP/IPMODEL

****

|  |  |  |
| --- | --- | --- |
| **S.No** | **OSIMODEL** | **TCP/IPMODEL** |
| 1 | Definedbeforeadventofinternet | DefinedaftertheadventofInternet. |
| 2 | Service interface and protocols areclearlydistinguishedbefore | Serviceinterfaceandprotocolswerenot clearly distinguished before |
| 3 | Internetworkingnotsupported | TCP/IPsupportsInternetworking |
| 4 | Strictlayering | Looselylayered |
| 5 | Protocolindependentstandard | ProtocolDependantstandard |
| 6 | LessCredible | MoreCredible |
| 7 | Allpacketsarereliablydelivered | TCPreliablydeliverspackets,IPdoes not reliably deliver packets |

**NETWORKPERFORMANCE**

Networkperformanceismeasuredinusing:

Bandwidth,Throughput,Latency,Jitter,RoundTripTime

### BANDWIDTH

* + Thebandwidthofanetworkisgivenbythenumberofbitsthatcanbetransmitted over the network in a certain period of time.
  + Bandwidthcanbemeasuredintwodifferentvalues:bandwidthinhertzand bandwidth in bits per second.

BandwidthinHertz

* Bandwidthinhertzreferstotherangeoffrequenciescontainedinacomposite signal or the range of frequencies a channel can pass.
* Forexample,wecansaythebandwidthofasubscribertelephonelineis4kHz.

BandwidthinBitsperSeconds

* Bandwidth inBitsperSecondsreferstothenumberofbitstransmittedper second.
* Forexample,thebandwidthofanetworkisamaximumof100Mbps.Thismeans that this network can send 100 Mbps.

Relationship

* There is an explicit relationship between thebandwidth in hertz andbandwidth in bits per second.
* Basically,anincreaseinbandwidthinhertzmeansanincreaseinbandwidth in bits per second.

### THROUGHPUT

* + Throughputisameasureofhowfastwecanactuallysenddatathrough a network.
  + Bandwidth in bits per second and throughput may seem to be same, but they are different.
  + A link may have a bandwidth of*B* bps, but we can only send *T* bps through thislink. (*T* always less than *B)*.
  + Inotherwords,thebandwidthisapotentialmeasurementofalink; the throughput is an actual measurement of how fast we can send data.
  + For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Problem:

Anetworkwithbandwidthof10Mbpscanpassonlyanaverageof12,000frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

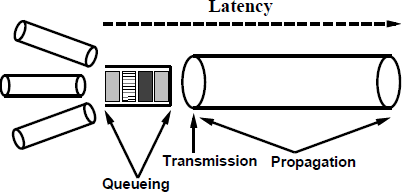
Solution

Wecancalculatethethroughput as

Thethroughputisalmostone-fifthofthebandwidthinthiscase.

### LATENCY(DELAY)

* + The latency or delay defines how long it takes for an entiremessage to travel from one end of a network to the other.
  + Latencyismadeupoffourcomponents:Propagationtime,Transmissiontime, Queuing time and Processing delay.



PropagationTime

* Propagation time measures the time required for a bit to travel fromthe source to the destination.
* Thepropagationtimeiscalculatedbydividing thedistancebythepropagation speed.
* The propagation speed of electromagnetic signals depends on the mediumand on the frequency of the signal.



TransmissionTime

* Indatacommunicationswedon’tsendjust1bit,wesendamessage.
* Thefirstbitmaytakeatimeequaltothepropagationtimetoreachitsdestination.
* Thelastbitalsomaytakethesameamountoftime.
* However, there is a time between the first bit leaving the sender and the last bitarriving at the receiver.
* Thefirstbitleavesearlierandarrivesearlier.
* Thelastbitleaveslaterandarriveslater.
* The transmission time of a message depends on the size of the message and thebandwidth of the channel.



QueuingTime

* Queuing time is the time needed for each intermediate or end device to hold themessage before it can be processed.
* Thequeuing timeisnotafixed factor.Itchangeswiththeloadimposedonthe network. When there is heavy traffic on the network, the queuing time increases.
* An intermediate device, such as a router, queues the arrived messages and processes them one by one.
* Iftherearemanymessages,eachmessagewillhavetowait.

ProcessingDelay

* Processingdelayisthetimethatthenodestaketoprocessthepacketheader.
* Processingdelayisakeycomponentinnetworkdelay.
* During processing of a packet, nodes may check for bit-level errors in the packet that occurred during transmission as well as determining where the packet's next destination is.

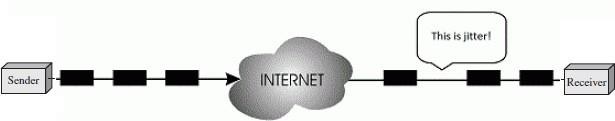
#### Bandwidth-DelayProduct

* Bandwidthanddelayaretwoperformancemetricsofalink.
* Thebandwidth-delayproductdefinesthenumberofbitsthatcanfillthe link.
* This measurement is important if we need to send data in bursts and wait for the acknowledgment of each burst before sending the next one.



### JITTER

* Anotherperformanceissuethatisrelatedtodelayisjitter**.**
* Jitter is a problem that if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio andvideo data, for example).
* If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.



### ROUND-TRIPTIME(RTT)

* RTT refers to how long it takes to send a message from one end of a network to the other and back, rather than the one-way latency. This is called as *round-trip time* (RTT) of the network.

### SOLVEDPROBLEMS–PERFORMANCE

Problem1:

Whatisthepropagationtimeifthedistancebetweenthetwopointsis12,000km? Assume the propagation speed to be 2.4 × 108m/s .

Solution:

Propagationtime=(12000\*1000)/(2.4×108)=50ms

Problem2:

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance betweenthesenderand thereceiver is 12,000 kmandthat light travels at

2.4\*108m/s.

Solution:

Propagationtime = (12000\*1000) /(2.4\*108)=50ms

Transmissiontime =(2500\*8)/109=0.02ms

Problem3:

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance betweenthesenderand thereceiver is 12,000 kmandthat light travels at

2.4\* 108m/s.

Solution:

Propagationtime=(12000\*1000)/(2.4\*108)=50ms

Transmissiontime =(5000000\*8)/106=40s

**UNITII :DATA-LINKLAYER&MEDIAACCESS**

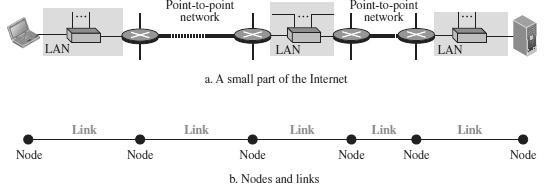
**Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP – Media Access Control – Wired LANs: Ethernet – Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices**

**1. INTRODUCTION**

* IntheOSImodel,thedatalinklayeristhe2ndlayerfromthebottom.
* Itisresponsiblefor**transmittingframesfromonenodetonextnode**.
* The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
* AnimportantcharacteristicofaDataLinkLayeristhatdatagram canbe handled by different link layer protocols on different links in a path.
* Theotherresponsibilitiesofthislayer are
  + **Framing -** Divides the stream of bits received into data units called frames.
  + **Physical addressing** – If frames are to be distributed to different systems on the same network, data link layer adds a header to the frame to define the sender and receiver.
  + **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow control mechanism.
  + **Error control**- Usedfor detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
  + **Medium Access control** - Used to determine which device has control over the link at any given time.

#### NodesandLinks

* Communicationatthedata-linklayerisnode-to-node.
* The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
* A data unit from one point in the Internet needs to pass through many networks (LAN and WAN) to reach another point.
* ThesesLANsandWANsareconnectedbyrouters.
* The two end hosts and the routers are ***nodes*** and the networks in- between are ***links*.**



* Thefirstnodeisthesourcehost;thelastnodeisthedestinationhost.
* Theotherfournodesarefourrouters.
* The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

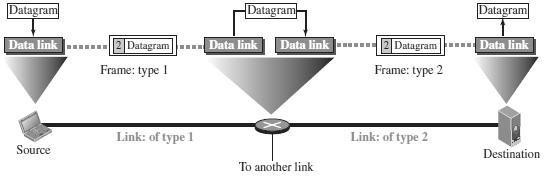
***TwoCategoriesofLinks***

Point-to-PointlinkandBroadcast link.

* Inapoint-to-pointlink,thelinkisdedicatedtothetwodevices
* Inabroadcastlink,thelinkissharedbetween severalpairsofdevices.

#### DataLinkLayer Services

* Thedata-linklayerislocatedbetweenthephysicalandthenetworklayers.
* The datalink layer provides services to the network layer; itreceives services from the physical layer.
* When a packet is travelling, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
* For this purpose, the data-link layer of the sending node needs to encapsulate the datagram and the data-link layer of thereceivingnode needs to decapsulate the datagram.



* The datagram received by the data-link layer of the source host is encapsulated in a frame.
* Theframeislogicallytransportedfromthesourcehosttotherouter.
* Theframeisdecapsulatedatthedata-linklayeroftherouterand encapsulated at another frame.
* Thenewframeislogicallytransportedfromtheroutertothedestination host.

#### SublayersinDataLinklayer

* Wecandividethedata-linklayerintotwosublayers:**datalinkcontrol (DLC)** and **media access control (MAC).**
* The data link control sublayer deals with all issues common to both point- to-point and broadcast links
* The media access control sublayer deals only with issues specific to broadcast links.

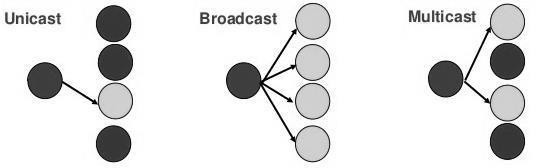


**2. LINK-LAYERADDRESSING**

* A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
* Since a linkis controlled at the data-linklayer, the addresses need tobelong to the data-link layer.
* When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.
* These two addresses are changed every time the frame moves fromone link to another.

### THREETYPESOFADDRESSES

Thelink-layerprotocolsdefinethreetypesofaddresses:unicast,multicast,and broadcast.



UnicastAddress:

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.

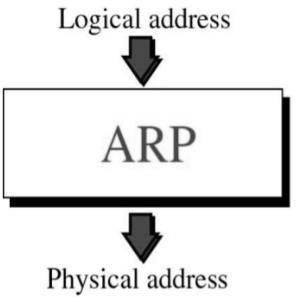
MulticastAddress:

Link-layer protocolsdefine multicastaddresses. Multicastingmeans one-to- many Communication but not all.

BroadcastAddress:

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.

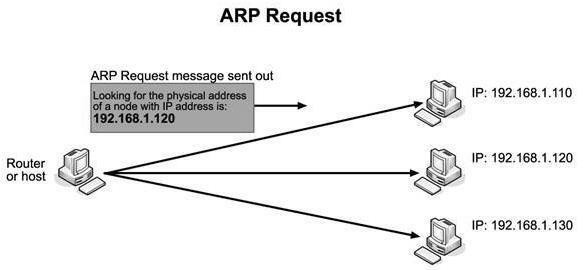
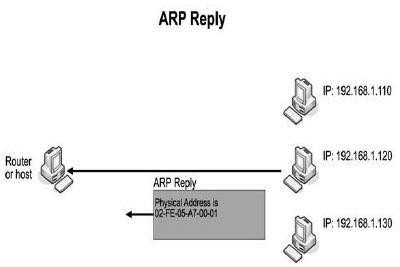
### ADDRESS RESOLUTIONPROTOCOL(ARP)

* ARPstandsforAddressResolutionProtocol.
* ARPisthemostimportantprotocoloftheDataLinkLayer.
* ****ARP is a network layer protocol used to **convert a IP address (Network/Logical address) into a MAC Address (Hardware /Physical address).**
* The computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens overthe physical address (MAC address).
* To send a datagram over a network, we need both the logical and physical address.
* IPaddressesare madeupof32bitswhereasMACaddressesare madeupof 48 bits.
* ARPenableseachhosttobuildatableofIPaddressandcorresponding physical address.
* ARPreliesonbroadcastsupportfromphysicalnetworks.
* TheAddressResolutionProtocolisarequestandresponseprotocol.
* ThetypesofARPmessagesare:
  1. ARPrequest
  2. ARPreply

#### ARPOperation

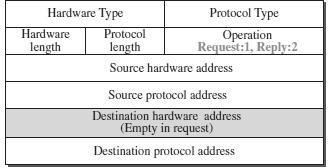
* ARP maintainsacachetableinwhichMACaddressesaremappedtoIP addresses.
* If ahostwantstosend anIPdatagramto ahost,itfirstchecksfora mapping in the cache table.
* If no mapping is found, it needs to invoke the Address Resolution Protocol over the network.
* ItdoesthisbybroadcastinganARPqueryontothenetwork.
* ThisquerycontainsthetargetIPaddress.
* EachhostreceivesthequeryandcheckstoseeifitmatchesitsIPaddress.
* Ifitdoesmatch,thehostsendsaresponsemessagethatcontainsitslink- layer address (MAC Address) back to the originator of the query.
* The originator adds the information contained in this response to its ARPtable.
* Forexample,

TodeterminesystemB’sphysical(MAC)address,systemAbroadcasts an ARP request containing B’s IP address to all machines on its network.



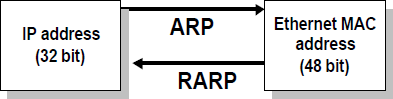
* AllnodesexceptthedestinationdiscardthepacketbutupdatetheirARP table.
* Destinationhost(SystemB)constructsanARPResponsepacket
* ARPResponseisunicastandsentbacktothesourcehost(SystemA).
* Source stores target Logical & Physical address pair in its ARP table from ARP Response.
* Iftargetnodedoesnotexistonsamenetwork,ARPrequestissentto default router.

#### ARPPacket

****

**RARP–Reverse ARP**

* ReverseAddress Resolution protocol (RARP)allows a host to convert its MAC address to the corresponding IP address.



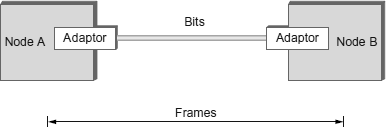
**3. DLCSERVICES**

* 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.
* Datalinkcontrolserviceinclude

**(1)Framing(2)FlowControl(3)Error Control**

### FRAMING

* + The data-link layerpacks thebits of a message into frames, so that eachframe is distinguishable from another.

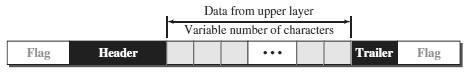


* + Although the whole message could be packed in one frame, that is not normally done.
  + One reason is that a frame can be verylarge, makingflow and error control very inefficient.
  + When a message is carried in one very large frame, even a single-bit errorwould require the retransmission of the whole frame.
  + Whenamessageisdividedintosmallerframes,asingle-biterroraffects only that small frame.
  + Framinginthedata-linklayerseparatesamessagefromonesourcetoa 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.

FrameSize

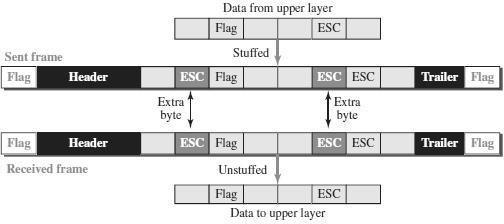
* + Framescanbeoffixedorvariablesize.
  + Frames of fixed size are called cells. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
  + In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Character-OrientedFraming

* + In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters.
  + To separate one frame from the next, an 8-bit (1-byte) flag is added at thebeginning and the end of a frame.
  + Theflag,composedofprotocol-dependentspecialcharacters,signalsthe start or end of a frame.
  + Anycharacterusedfortheflagcouldalsobepartoftheinformation.
  + If this happens, when it encounters this pattern in the middle of the data,the receiverthinks it has reached the end of the frame.
  + To fix this problem, a **byte-stuffing** strategy was added to character- oriented framing.

***ByteStuffing(or)CharacterStuffing***

* + Bytestuffingistheprocessofaddingoneextrabyte whenever thereisa flag or escape character in the text.
  + Inbytestuffing,aspecialbyteisaddedtothedatasectionoftheframe when there is a character with the same pattern as the flag.
  + The data sectionis stuffedwith anextrabyte. This byte isusually called the escape character (ESC) and has a predefined bit pattern.
  + Whenever the receiver encounters the ESC character, it removes it fromthe data section and treats the next character as data, not as a delimiting flag.



Bit-OrientedFraming

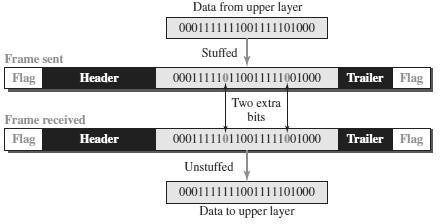
* + In bit-oriented framing, the data section of a frame is a sequence of bits tobe interpreted by the upper layer as text, graphic, audio, video, and so on.
  + In addition to headers and trailers), we still need a delimiter to separate one frame from the other.
  + Mostprotocolsuseaspecial8-bitpatternflag,01111110, asthedelimiterto define the beginning and the end of the frame



* + Iftheflagpatternappearsinthedata,thereceiver mustbeinformedthat this is not the end of the frame.
  + Thisisdonebystuffing1singlebit(insteadof1byte)topreventthepattern from looking like a flag. The strategy is called **bit stuffing.**

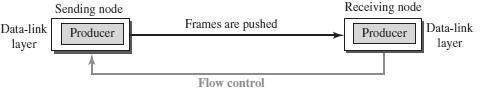
***BitStuffing***

* + Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.
  + In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.
  + Thisextrastuffedbitiseventuallyremovedfromthedatabythereceiver.
  + The extra bit is added after one 0 followed by five 1’s regardless of the value of the next bit.
  + This guarantees that the flagfield sequence does not inadvertently appear in the frame.



### FLOWCONTROL

* Flow control refers to a set of procedures used to restrictthe amount of data that the sender can sendbefore waiting for acknowledgment.
* Thereceivingdevicehaslimitedspeedandlimitedmemorytostorethe data.
* Therefore,thereceivingdevicemustbeableto informthesendingdeviceto stop the transmission temporarily before the limits are reached.
* Itrequiresabuffer, ablockof memoryforstoringtheinformationuntilthey are processed.

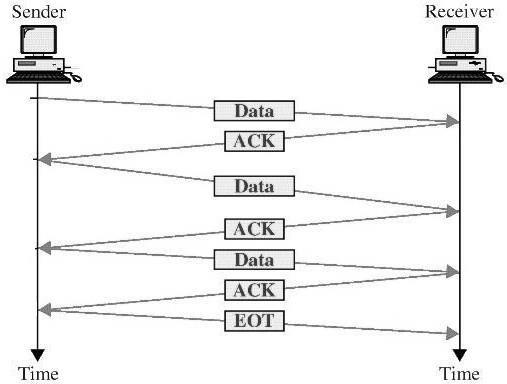


Twomethodshave beendevelopedtocontroltheflowofdata:

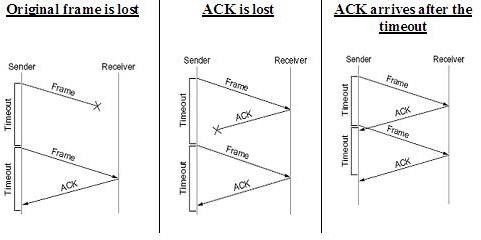
* Stop-and-Wait
* SlidingWindow

STOP-AND-WAIT

* Thesimplestschemeisthestop-and-waitalgorithm.
* IntheStop-and-waitmethod,thesenderwaitsforanacknowledgement after every frame it sends.
* Whenacknowledgementisreceived,thenonlynextframeissent.
* The processofalternately sending andwaiting ofa framecontinuesuntil the sender transmits the EOT (End of transmission) frame.



* If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.
* The acknowledgement may not arrive because of the following three scenarios :
  1. Originalframeislost
  2. ACKislost
  3. ACKarrivesafterthetimeout



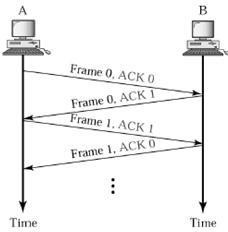
AdvantageofStop-and-wait

* TheStop-and-waitmethodissimpleaseachframeischeckedand acknowledged before the next frame is sent

DisadvantagesofStop-And-Wait

* In stop-and-wait,atany pointin time,there isonly one frame thatis sent and waiting to be acknowledged.
* Thisisnotagooduseoftransmissionmedium.
* To improve efficiency, multiple frames should be in transition while waiting for ACK.

PIGGYBACKING



* A method to combine a data frame with ACK.
* Piggybackingsavesbandwidth
* Station A and B both have data to send.
* Instead of sending separately, station A sends a data frame that includes an ACK.
* StationBdoesthesamething.

**SLIDINGWINDOW**

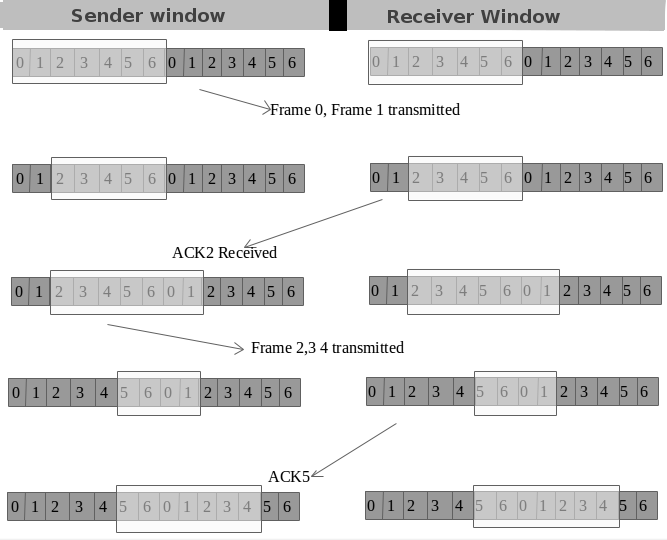
* The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
* In Sliding Window Control, multiple frames can be sent one after the another due towhichcapacity ofthecommunication channel canbeutilized efficiently.
* AsingleACKacknowledgemultipleframes.
* Sliding Window refers to imaginary boxes at both the sender and receiver end.
* The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
* Frames can be acknowledged even when the window is not completely filled.
* The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1.
* Forexample,ifn=8,theframesarenumbered from

0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1........

* Thesizeofthewindowisrepresentedasn-1.Therefore,maximumn-1 frames can be sent before acknowledgement.
* When the receiver sends the ACK, it includes the number of the next frame that it wants to receive.
* For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5.
* When the sender sees the ACK with the number 5, it got to know that theframes from 0 through 4 have been received.

|  |  |
| --- | --- |
| **SenderWindow** | **ReceiverWindow** |
|  |  |
| * Atthebeginningofatransmission,the sender window contains n-1 frames. * When a frame is sent, the size of the window shrinks. * For example, ifthe sizeofthewindow is ‘w’ and if three frames are sent out, then the number of frames left out in the sender window is w-3. * Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK. | * At the beginning of transmission, the receiverwindowdoesnotcontainnframes, but it contains n-1 spaces for frames. * When thenewframearrives, thesizeofthe window shrinks. * For example, the size of the window is w and if three frames are received then the number of spaces available in the windowis (w-3). * Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged. |

**ExampleofSlidingWindow**

****

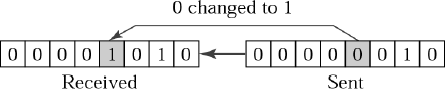
### ERROR CONTROL

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error Control is a technique of error detection and retransmission.

TYPESOFERRORS

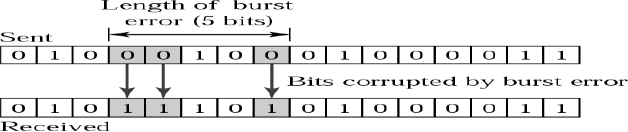
**SINGLE-BITERROR**

ThetermSingle-biterror meansthatonlyonebitofagivendataunit(suchasbyte, character, data unit or packet) is changed from 1 to 0 or from 0 to 1.



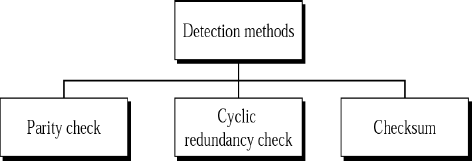
BURSTERROR

Theterm BurstErrormeansthattwoormorebitsinthedataunithavechanged from 1 to 0 or from 0 to 1.



ERRORDETECTIONTECHNIQUES/METHODS

The basic idea behind any error detection scheme is to add additional information to a frame that can be used to determine if errors have been introduced.



**PARITY CHECK**

* One bit, called paritybit is added to everydata unit so that the total number of 1’s in the data unit becomes even (or) odd.
* Thesourcethentransmitsthisdataviaalink,andbitsarecheckedand verified at the destination.
* Data is considered accurate if the number of bits (even or odd) matches the number transmitted from the source.
* Thistechniquesisthemostcommonandleastcomplex method.

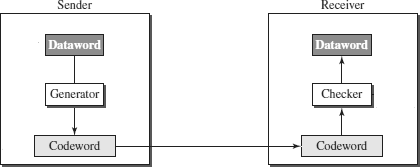
1. ***Evenparity***–Maintainevennumberof1s E.g., 1011 → 1011 **1**
2. ***Oddparity***–Maintainoddnumberof1s E.g., 1011 → 1011 **0**

**CYCLICREDUNDANCYCHECK**

* Cyclic codes refers to encoding messages by adding a fixed-length check value.
* CRCs are popular because they are simple to implement, easy to analyze mathematically and particularly good at detecting common errors caused in transmission channels.

StepsInvolved:

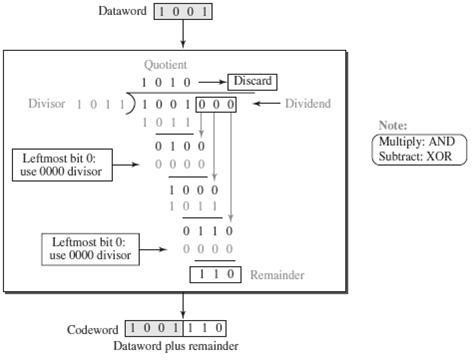
* Consider the original message (dataword) as M(x) consistingof ‘k’bits and the divisor as C(x) consists of‘n+1’bits.
* TheoriginalmessageM(x)isappendedby ‘n’bitsofzero’s.Letuscall this zero-extendedmessage as T(x).
* DivideT(x)byC(x)andfindtheremainder.
* ThedivisionoperationisperformedusingXORoperation.
* The resultant remainder is appended to the original message M(x) as CRC and sentby the sender(codeword).



Example1:

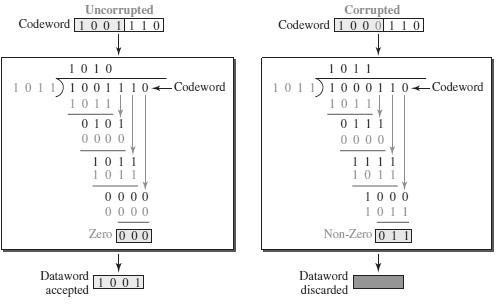
* ConsidertheDataword/MessageM(x)=1001
* DivisorC(x)=1011(n+1=4)
* Appending‘n’zerostotheoriginalMessageM(x).
* TheresultantmessagesiscalledT(x)=1001**000.**(heren=3)
* DivideT(x)bythedivisorC(x)usingXORoperation.

***SenderSide:***

******

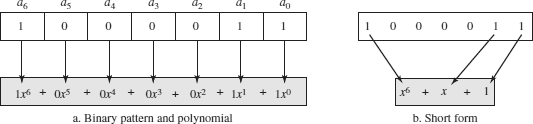
***ReceiverSide:***

(ForBothCase–WithoutErrorandWithError)

****

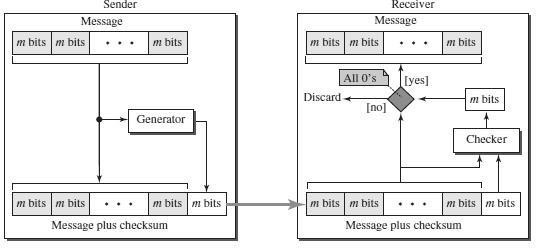
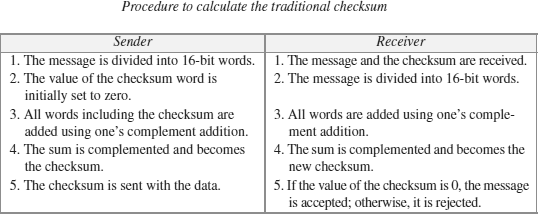
**Polynomials**

* Apattern of 0s and 1s can be represented as a **polynomial** with coefficients of 0 and 1.
* The power of each termshows the position of the bit; the coefficient shows the value of the bit.

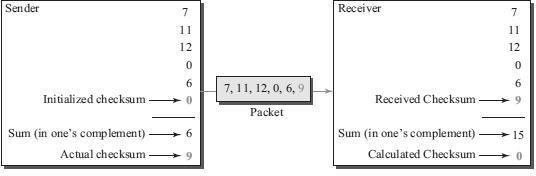


INTERNETCHECKSUM

* Checksumisacalculatedvaluethatisusedtodeterminetheintegrityof data.



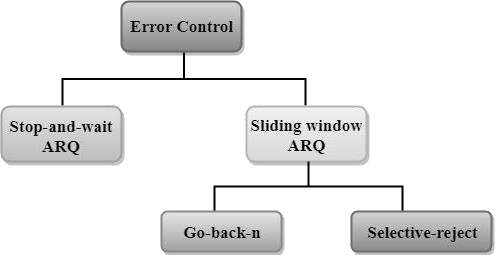
**Example:**Letthemessagetobetransmittedbe7,11,12,0,6.



### ERRORCONTROL

* Errorcontrolincludesbotherrordetectionanderrorcorrection.
* Wheneveranerrorisdetected,specifiedframesareretransmitted
* It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender.
* Includesthefollowingactions:
  + Errordetection
  + PositiveAcknowledgement(**ACK**):iftheframearrivedwithno errors
  + NegativeAcknowledgement(**NAK**):iftheframearrivedwitherrors
  + Retransmissions after **Timeou**t: Frame is retransmitted after certain amount of time if no acknowledgement was received
* Errorcontrolinthedatalinklayerisbasedonautomaticrepeatrequest (ARQ).

**CategoriesofErrorControl**

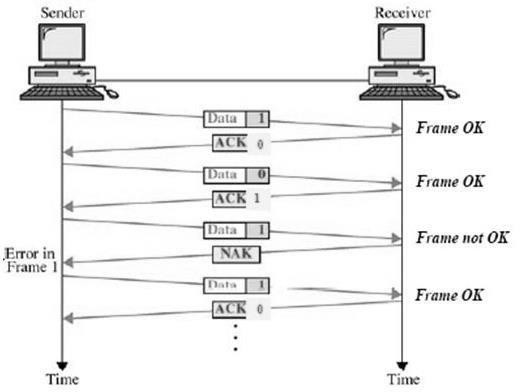
****

STOP-AND-WAITARQ

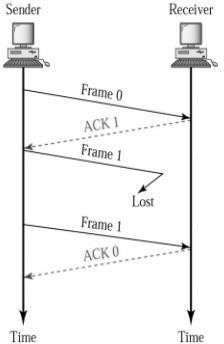
* Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.
* This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

TwopossibilitiesoftheretransmissioninStopandWait ARQ:

* **Damaged Frame:** When the receiver receives a damaged frame(i.e., the frame contains an error), then it returns the NAK frame. For example, when the frame DATA 1 is sent, and then the receiver sends the ACK 0 frame means that the data 1 has arrived correctly. The sender transmits the next frame: DATA 0. It reaches undamaged, and the receiver returns ACK 1.Thesendertransmitsthethirdframe:DATA1. Thereceiverreportsanerror and returns the NAK frame. The sender retransmits the DATA 1 frame.



* **Lost Frame:** Sender is equipped withthe timer andstarts whentheframe is transmitted. Sometimes the frame has not arrived at the receivingend so that it cannot be acknowledged either positively or negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.



SLIDINGWINDOWARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

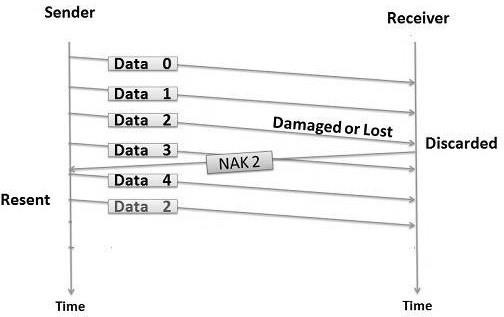
TwoprotocolsusedinslidingwindowARQ:

1. **GO-BACK-NARQ**
   * InGo-Back-NARQprotocol,ifoneframeislostordamaged,thenitretransmits all the frames after which it does not receive the positive ACK.



* + In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.
  + ThereceiverdiscoverstheerrorinData2frame,soitreturnstheNAK2 frame.
  + All the frames including the damaged frame (Data 2,3,4) are discarded as it is transmitted after the damaged frame.
  + Therefore,thesenderretransmitstheframes(Data2,3,4).

1. **SELECTIVE-REJECT(REPEAT)ARQ**
   * Selective-RejectARQtechniqueismoreefficientthanGo-Back-nARQ.
   * Inthistechnique,onlythoseframesareretransmittedforwhichnegative acknowledgement (NAK) has been received.
   * The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
   * The receiver must have an appropriate logic for reinserting the frames in a correct order.
   * Thesendermustconsistofasearchingmechanismthatselectsonlythe requested frame for retransmission.

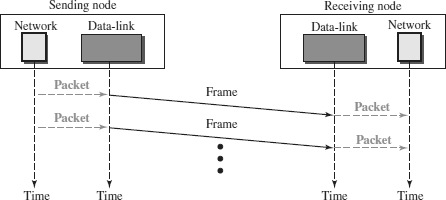


* + In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.
  + The receiverdiscoverstheerror inData 2frame,soit returnsthe NAK2 frame.
  + Thedamagedframeonly(Data2)isdiscarded.
  + Theothersubsequentframes(Data3,4)areaccepted.
  + Therefore,thesenderretransmitsonlythedamagedframe(Data2).

**4. DATA-LINKLAYERPROTOCOLS**

Fourprotocolshavebeendefinedforthedata-linklayercontrols. They are

1. SimpleProtocol
2. Stop-and-WaitProtocol
3. Go-Back-NProtocol
4. Selective-RepeatProtocol
5. SIMPLEPROTOCOL
   * Thefirstprotocolisasimpleprotocolwithneitherflownorerrorcontrol.
   * Weassumethatthereceivercanimmediatelyhandleanyframeitreceives.
   * Inotherwords,thereceivercanneverbeoverwhelmedwithincoming frames.
   * The data-link layersof the sender and receiver provide transmissionservices for their network layers.



* + Thedata-linklayeratthesendergetsapacket fromitsnetworklayer,makes a frame out of it, and sends the frame.
  + The data-link layer at the receiver receives a frame from the link, extractsthe packet from the frame, and delivers the packet to its network layer.

**NOTE:**

1. **STOP-AND-WAITPROTOCOL**

REFERSTOPANDWAITFROMFLOWCONTROL

1. **GO-BACK-N PROTOCOL**

REFERGO-BACK-NARQFROMERRORCONTROL

1. **SELECTIVE-REPEAT PROTOCOL**

REFERSELECTIVE-REPEATARQFROMERRORCONTROL

**5. HDLC(HIGH-LEVELDATALINKCONTROL)**

* + High-levelDataLinkControl(HDLC)isabit-orientedprotocol
  + HDLCisusedforcommunicationoverpoint-to-pointandmultipointlinks.
  + HDLCimplementstheStop-and-Waitprotocol.

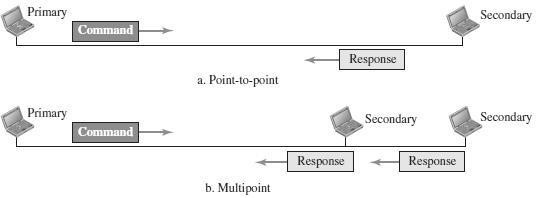
HDLCCONFIGURATIONSANDTRANSFERMODES

HDLCprovidestwocommontransfer modesthatcanbeusedindifferent configurations:

1. Normalresponsemode(NRM)
2. Asynchronousbalancedmode(ABM).

***Normalresponsemode(NRM)***

* + Innormalresponsemode(NRM),thestationconfigurationisunbalanced.
  + Wehaveoneprimarystationandmultiplesecondarystations.
  + A*primarystation*cansendcommands;a*secondarystation*canonly respond.
  + TheNRMisusedforbothpoint-to-pointandmultipointlinks.



***Asynchronousbalancedmode(ABM)***

* + InABM,theconfigurationisbalanced.
  + Thelinkispoint-to-point,andeachstationcanfunctionasa primaryanda secondary (acting as peers).
  + Thisisthecommon modetoday.



HDLCFRAMES

HDLCdefinesthreetypesofframes:

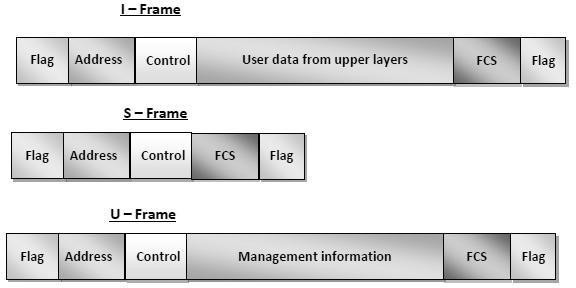
1. Informationframes(I-frames)-usedtocarryuserdata
2. Supervisoryframes(S-frames)-usedtocarrycontrolinformation
3. Unnumberedframes(U-frames)–reservedforsystemmanagement

Eachtypeof frameservesas anenvelopeforthetransmissionof adifferenttypeof message.

EachframeinHDLCmaycontainuptosixfields:

1. Beginningflagfield
2. Addressfield
3. Controlfield
4. Informationfield(UserInformation/ManagementInformation)
5. Framechecksequence(FCS)field
6. Endingflagfield

Inmultiple-frametransmissions,theendingflagofoneframecanserveasthe beginning flag of the next frame.



* + ***Flag field -*** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
  + ***Address field -*** This field contains the address of the secondary station. If a primary station created the frame, it contains a ‘*to’* address. If a secondary station creates the frame, it contains a ‘*from’* address. The address field can be one byte or several bytes long, depending on the needs of the network.
  + ***Control field.*** The control field is one or two bytes used for flow and error control.
  + ***Information field.*** The information field contains the user’s data from the network layer or management information. Its length can vary from one network to another.
  + ***FCS field.*** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 16- bit or 32-bit CRC.

**CONTROLFIELDFORMATFORTHEDIFFERENTFRAMETYPES**

***ControlFieldforI-Frames***

* + I-frames are designed to carry user data fromthe networklayer. In addition, they can include flow-control and error-control information



* + Thefirstbitdefinesthetype.Ifthefirstbitofthecontrolfieldis0,this means the frame is an I-frame.
  + Thenext3bits,calledN(S),definethesequencenumberoftheframe.
  + Thelast3bits,calledN(R),correspondtotheacknowledgmentnumber when piggybacking is used.
  + The single bit between N(S) and N(R) is called the P/F bit. If this bit is1 it meanspoll (the frame is sent by a primary station to a secondary).
  + Ifthisbitis0itmeansfinal(theframeissentbyasecondarytoaPrimary).

***ControlFieldforS-Frames***

* + Supervisoryframes areused forflow anderrorcontrol whenever piggybacking is either impossible or inappropriate.
  + S-framesdonothaveinformationfields



* + If the first 2 bits of the control field are 10, this means the frame is an S- frame.
  + The last 3 bits, called N(R),correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK), dependingon thetype of S-frame.
  + The2bitscalledcodeareusedtodefinethetypeofS-frameitself.
  + With2bits,wecanhavefourtypesofS-frames–

Receive ready (RR), Receive not ready (RNR), Reject (REJ) and Selective reject (SREJ).

***ControlFieldforU-Frames***

* + Unnumbered frames are used to exchange session management and control information between connected devices.
  + U-frames contain an information field, but used only for system management information andnot user data.



* + Ifthefirst 2 bitsofthe controlfield are11,thismeans theframe is anU- frame.
  + U-frame codes are divided into two sections: a 2-bit prefix before the P/Fbit and a 3-bit suffix after the P/F bit.
  + Together, these two segments (5 bits)can beused to create upto 32 different types of U-frames.

**6. POINT-TO-POINTPROTOCOL(PPP)**

* + Point-to-PointProtocol(PPP)wasdevisedbyIETF(InternetEngineering Task Force) in 1990 as a Serial Line Internet Protocol (SLIP).
  + PPP is adata link layercommunications protocolused to establish a direct connection between two nodes.
  + It connectstwo routers directly withoutany host or any other networkingdevice in between.
  + ItisusedtoconnecttheHomePCtotheserverofISP viaamodem.
  + Itisabyte-orientedprotocolthatiswidelyusedinbroadband communications having heavy loads and high speeds.
  + Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

#### ServicesProvidedbyPPP

ThemainservicesprovidedbyPoint-to-PointProtocolare−

1. Definingtheframeformatofthedatatobetransmitted.
2. Definingtheprocedureofestablishinglinkbetweentwopointsand exchange of data.
3. Statingthe methodofencapsulationofnetworklayerdataintheframe.
4. Statingauthenticationrulesofthecommunicatingdevices.
5. Providingaddressfornetworkcommunication.
6. Providingconnectionsovermultiplelinks.
7. Supportingavarietyofnetworklayerprotocolsbyprovidingarangeos services.

#### PPPFrame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes.



1. **Flag**−1bytethatmarksthebeginningandtheendoftheframe. Thebit pattern of the flag is 01111110.
2. **Address**−1bytewhichissetto11111111incaseofbroadcast.
3. **Control**−1bytesettoaconstantvalueof11000000.
4. **Protocol** −1or2bytesthatdefinethetypeofdatacontainedinthepayload field.
5. **Payload**−Thiscarriesthedatafromthenetworklayer. Themaximum length of the payload field is 1500 bytes.
6. **FCS**−Itisa2byte(16-bit)or4bytes(32-bit)framechecksequencefor error detection. The standard code used is CRC.

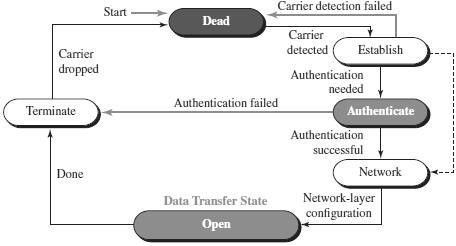
#### ByteStuffinginPPPFrame

Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removesthe escape byte before passing it onto the network layer.

#### TransitionPhasesinPPP

ThePPPconnectiongoesthroughdifferentstatesasshownina*transitionphase*

diagram.



* + **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.
  + **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase.
  + **Authenticate**: This phase is optional. The two nodes may decide whether they need this phase during the establishment phase. If they decide to proceed with authentication, they send several authentication packets. If the result is successful, theconnection goes to thenetworkingphase; otherwise, it goes to the termination phase.
  + **Network**: In network phase, negotiation for the network layer protocols takes place.PPP specifies that two nodes establish a networklayer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.
  + **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.
  + **Terminate**:Inthisphaseconnectionisterminated.

#### Components/ProtocolsofPPP

Threesetsofcomponents/protocolsaredefinedtomakePPPpowerful:

* + LinkControlProtocol (LCP)
  + AuthenticationProtocols(AP)
  + NetworkControlProtocols(NCP)

**Link Control Protocol (LCP)**− It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established.

**Authentication Protocols (AP)**− Authentication means validating the identity ofa user who needs to access a set of resources. PPP has created two protocols for authentication -Password Authentication Protocol and Challenge Handshake Authentication Protocol.

PAP

The Password Authentication Protocol (PAP) is a simple authentication procedure with a two-step process:

1. Theuserwhowantstoaccessasystemsendsanauthentication identification (usually the user name) and a password.
2. Thesystemchecksthevalidityoftheidentificationandpasswordand either accepts or denies connection.

CHAP

The Challenge Handshake Authentication Protocol (CHAP) is a three-way handshakingauthentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.

1. Thesystemsendstheuserachallengepacketcontainingachallenge value.
2. The user applies a predefined function that takes the challenge value and theuser’sownpasswordandcreatesa result.Theusersendstheresultin theresponse packet to the system.
3. Thesystemdoesthesame.Itappliesthesame functiontothepasswordof the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

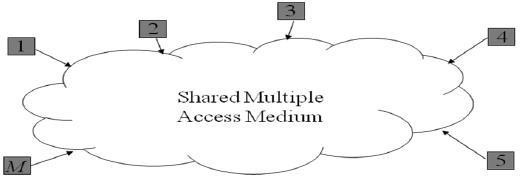
CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.

**Network Control Protocols (NCP)**−PPP is a multiple-network-layer protocol. It cancarryanetwork-layerdatapacketfrom protocolsdefinedbytheInternet.PPP

has defined a specific Network Control Protocol for each network protocol. These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there.

**7. MEDIAACCESSCONTROL(MAC)**

* Whentwoormorenodestransmitdataatthesametime,theirframeswill collide and the link bandwidth is wasted during collision.
* Tocoordinatetheaccessofmultiplesending/receivingnodestotheshared link, we need a protocol to coordinate the transmission.
* TheseprotocolsarecalledMediumorMultipleAccessControl(MAC) Protocols. MAC belongs to the data link layer of OSI model
* MAC defines rules for orderly access to the shared medium. It tries to ensurethatnotwonodesareinterferingwitheachother’stransmissions, and deals with the situation when they do.



IssuesinvolvedinMAC

Thekeyissuesinvolvedare–

* + ***Where***thecontrolisexercised-referstowhetherthecontrolisexercised in a centralized or distributed manner
  + ***How***thecontrolisexercised-referstoinwhatmannerthecontrolis exercised

GoalsofMAC

1. Fairnessinsharing
2. Efficientsharingofbandwidth
3. Needtoavoidpacketcollisionsatthereceiverduetointerference

MACManagement

* + Mediumallocation(collisionavoidance)
  + Contentionresolution(collisionhandling)

MACTypes

* **Round-Robin:**–Eachstationisgivenopportunitytotransmitinturns. Either a central controller polls a station to permit to go, or stations can coordinate among themselves.
* **Reservation: -** Station wishingto transmit makes reservations for time slots in advance. (Centralized or distributed).
* **Contention(RandomAccess)**:-Nocontrolonwhotries;Ifcollision‖ occurs, retransmission takes place.

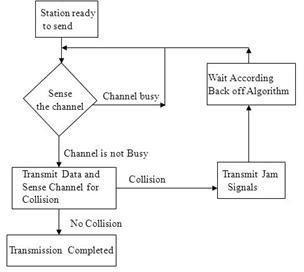
MECHANISMSUSED

* + WiredNetworks:
    - CSMA/CD–CarrierSenseMultipleAccess/CollisionDetection
  + WirelessNetworks:
    - CSMA/CA–CarrierSenseMultipleAccess/CollisionAvoidance

CARRIERSENSEMULTIPLEACCESS/COLLISIONDETECTION(CSMA / CD)

* **Carrier Sense** in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.
  + Ifthecarriersensedisidle,thenthenodetransmitstheentire frame.
  + Ifthecarriersensedisbusy,thetransmissionispostponed.
* **Collision Detect** means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

**FlowchartofCSMA/CDOperation**

****

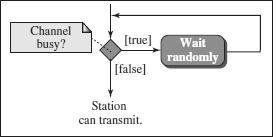
#### TransmitterAlgorithminCSMA/CD

* TransmitterAlgorithmdefinestheproceduresforanodethatsensesabusy medium.
* ThreetypesofTransmitterAlgorithmexist**.**
* Theyare

1. Non-PersistentStrategy
2. PersistentStrategy:1-Persistent&P-Persistent

Non-PersistentStrategy

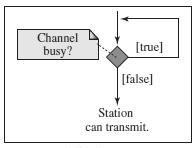
* In the non-persistent method,a station that has a frame to send senses theline.
* Ifthelineisidle,itsendsimmediately.
* If the line is not idle, it waits a random amount of time and then senses the line again.



* The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
* However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

PersistentStrategy

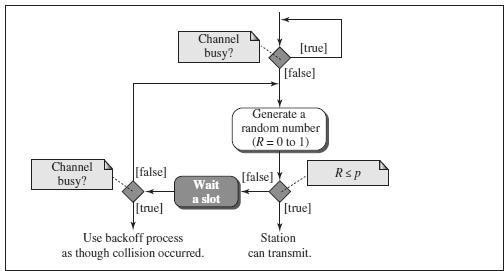
1. ***Persistent:***
   * The1-persistentmethodissimpleandstraightforward.
   * In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).



* + This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

***P-Persistent:***

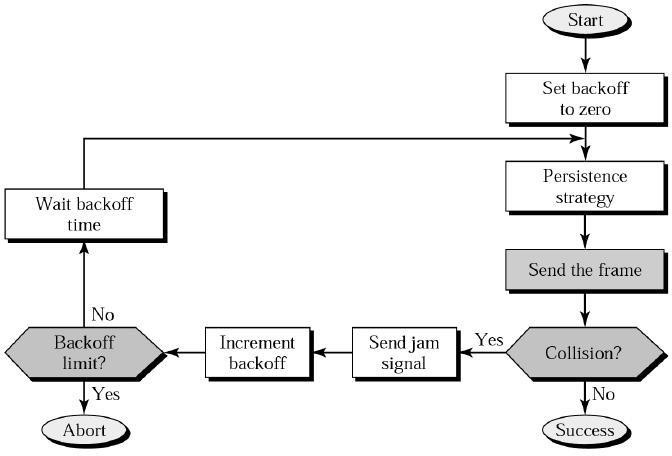
* + Inthismethod,afterthestationfindsthelineidleitfollowsthesesteps:
  + Withprobability*p*,thestationsendsitsframe.
  + Withprobability *q*= 1− *p*, thestation waits forthebeginning ofthenext time slot and checks the line again.



* + Thep-persistentmethodisusedifthechannelhastimeslotswithaslot duration equal to or greater than the maximum propagation time.
  + The p-persistent approach combines theadvantages ofthe other two strategies. It reduces the chance of collision and improves efficiency.

.

EXPONENTIALBACK-OFF

* + Oncean adaptorhas detected acollisionandstopped its transmission, it waits acertain amount of time and tries again.
  + Eachtime it tries to transmit but fails,the adaptor doubles theamount of time it waits before trying again.
  + ****Thisstrategyofdoublingthedelayintervalbetweeneachretransmission attempt is a general technique known as **exponential back-off.**

CARRIERSENSEMULTIPLEACCESS/COLLISIONAVOIDANCE(CSMA/CA)

* + Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.
  + Wireless protocol would follow exactly the same algorithm as the Ethernet—Wait until the linkbecomes idle before transmittingand backoff should a collision occur.
  + Collisions are avoided through the use of CSMA/CA’s three strategies: the interframe space, the contention window, and acknowledgments

***Interframe Space (IFS) -*** First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the ***interframe space*** or ***IFS*.**

***Contention Window -*** The **contention window** is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFStime.

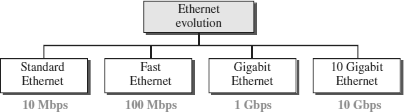
***Acknowledgment -*** In addition, the data may be corrupted during the transmission.The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

**8. WIREDLAN:ETHERNET(IEEE802.3)**

* + Ethernetwasdevelopedinthemid-1970’sattheXeroxPaloAltoResearch Center (PARC),
  + IEEEcontrolstheEthernetstandards.
  + The Ethernet is the most successful local area networking technology, that uses bus topology.
  + TheEthernetis**multiple-accessnetworks**thatissetofnodessendand receive frames over a shared link.
  + Ethernetusesthe**CSMA/CD(C**arrier**S**ense**M**ultiple**A**ccesswith

**C**ollision**D**etection)mechanism.

**EVOLUTIONOFETHERNET**

****

##### StandardEthernet(10Mbps)

TheoriginalEthernettechnologywiththedatarateof10MbpsastheStandard Ethernet.

StandardEthernettypesare

1. 10Base5:ThickEthernet,
2. 10Base2:ThinEthernet,
3. 10Base-T:Twisted-PairEthernet
4. 10Base-F:FiberEthernet.

|  |  |
| --- | --- |
| **10Base5:ThickEthernet**     * The first implementation is called ***10Base5, thick Ethernet,*** or ***Thicknet.*** * 10Base5 was the first Ethernet specificationtouseabustopology with an external **transceiver**(transmitter/receiver) connected via a tap to a thick coaxial cable. | **10Base2:ThinEthernet**     * The second implementation iscalled ***10Base2, thin Ethernet,*** or ***Cheapernet.*** * 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. * In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station. |
| **10Base-T:Twisted-PairEthernet**     * Thethirdimplementationiscalled   ***10Base-T***or***twisted-pairEthernet.***   * 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable. | **10Base-F:FiberEthernet**     * Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called ***10Base-F.*** * 10Base-F uses a star topology to connect stations to a hub. * The stations are connected tothe hub using two fiber-optic cables. |

##### FastEthernet(100Mbps)

Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.

The100BASE-Tstandardconsistsofthreedifferentcomponentspecifications–

1. 100 BASE-TX
2. 100BASE-T4
3. 100BASE-FX

|  |  |  |
| --- | --- | --- |
| **100BASE-TX** | **100BASE-T4** | **100BASE-FX** |
| **100Base-TX** uses two pairs of twisted-paircable either UTP or STP. A 100Base-TX network can provide a data rate of 100 Mbps. | A new standard, called ***100Base-T4,*** was designed to use four pairs of UTP for transmitting 100 Mbps. | **100Base-FX** uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements. |

##### GigabitEthernet(1Gbps)

* + TheGigabitEthernetupgradesthedatarateto1Gbps(1000Mbps).
  + GigabitEthernetcanbecategorizedaseitheratwo-wireorafour-wire implementation.
  + The two-wire implementations use fiber-optic cable (**1000Base-SX,** short- wave, or **1000Base-LX,** long-wave), or STP (**1000Base-CX**).
  + Thefour-wireversionusescategory5twisted-paircable(**1000Base-T**).

##### 10GigabitEthernet(10Gbps)

* + 10Gigabit Ethernet is anupcomingEthernettechnologythattransmitsat10 Gbps.
  + 10GigabitEthernetenablesafamiliarnetworktechnologytobeusedin LAN, MAN and WAN architectures.
  + 10GigabitEthernetusesmultimodeopticalfiberupto300metersand single mode fiber up to 40 kilometers.
  + Four implementations are the most common:**10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4.**

ACCESSMETHOD/PROTOCOLOFETHERNET

TheaccessmethodofEthernetisCSMA/CD.

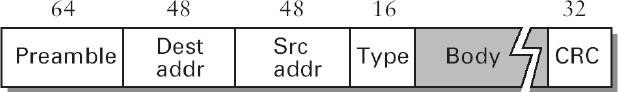
## Note:ReferCSMA/CDfromMAC

COLLISIONDETECTIONINETHERNET

* + - As the Ethernet supports collision detection, senders are able to determine a collision.
    - At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a **32-bit jamming sequence** alongwith the **64- bit preamble** (totally 96 bits) and then stops the transmission.
    - These**96bits**aresometimescalled**RuntFrame.**

FRAMEFORMATOFETHERNET

TheEthernetframeisdefinedbytheformatgiveninthe Fig.



* The 64-bit ***preamble*** allows thereceiver to synchronize with the signal; it is a sequence of alternating 0’s and 1’s.
* Boththe***sourceanddestination***hostsareidentifiedwitha48-bit***address.***
* Thepacket***type***fieldservesasthedemultiplexingkey.
* Eachframecontainsupto1500bytesof***data(Body).***
* ***CRC***isusedforErrordetection

EthernetAddresses

* EveryEthernethosthasauniqueEthernetaddress(48bits–6bytes).
* Ethernetaddressisrepresentedbysequenceofsixnumbersseparatedby colons.
* Eachnumbercorrespondsto1byteofthe6byteaddressandisgivenby pair of hexadecimal digits.
* **Eg:8:0:2b:e4:b1:2**istherepresentationof

000010000000000000101011111001001011000100000010

* Each frame transmitted on an Ethernet is received by every adaptorconnected to the Ethernet.
* In addition to ***unicast*** addresses an Ethernet address consisting of ***all 1s*** istreated as ***broadcast*** address.
* Similarly the address that has the ***first bit set to 1*** but it is not the broadcast address is called ***multicast*** address.

ADVANTAGESOFETHERNET

Ethernetsaresuccessfulbecause

* Itisextremely***easytoadministerandmaintain.*** Therearenoswitchesthat can fail, no routing or configuration tables that have to be kept up-to-date, and it is easy to add a new host to the network.
* Itis***inexpensive:***Cableischeap,andtheonlyothercostisthenetwork adaptor on each host.

**9. WIRELESSLAN(IEEE802.11)**

* + Wirelesscommunicationisoneofthefastest-growingtechnologies.
  + 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.

**ADVANTAGESOFWLAN/802.11**

1. **Flexibility:**Withinradiocoverage,nodescanaccesseachotherasradio wavescan penetrate evenpartition walls.
2. **Planning:** No prior planningisrequired forconnectivityaslongas devices follow standard convention
3. **Design:**Allowstodesignanddevelopmobiledevices.
4. **Robustness :** Wireless networkcan survive disaster. If the devices survive, communicationcan still be established.

DISADVANTAGESOF WLAN/802.11

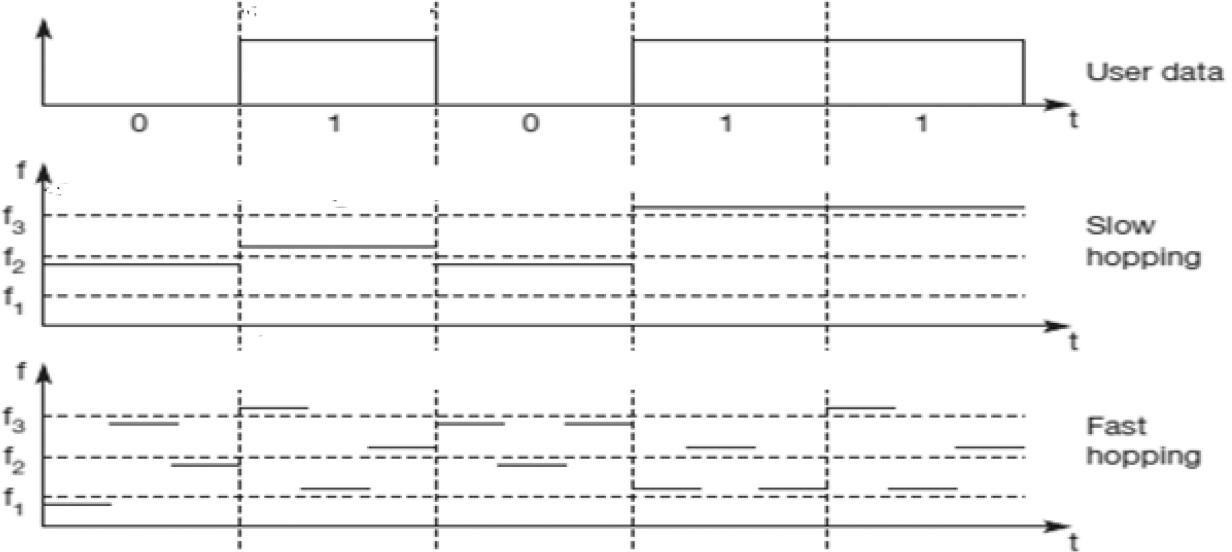
1. **Quality of Service :** Low bandwidth (1 – 10 Mbps), higher error rates due to interference, delay due to error correction and detection.
2. **Cost:**WirelessLANadaptersarecostlycomparedtowiredadapters.
3. **Proprietary Solution:** Due to slow standardization process, many solution are proprietary that limit the homogeneity of operation.
4. **Restriction :** Individual countries have their own radio spectral policies. This restricts the development of the technology
5. **Safety and Security :** Wireless Radio waves may interfere with other devices. Eg; In a hospital, radio waves may interfere with high-tech equipment.

**TECHNOLOGYUSEDINWLAN/802.11**

* + WLAN’susesSpreadSpectrum(SS)technology**.**
  + The idea behind Spread spectrum technique is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.
  + TherearetwotypesofSpread Spectrum:
    - FrequencyHoppingSpreadSpectrum(FHSS)
    - Direct**S**equenceSpreadSpectrum(DSSS)

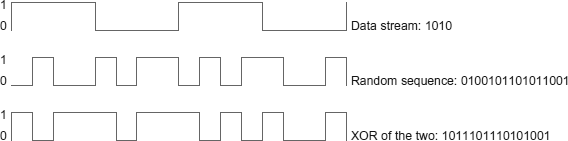
**FrequencyHoppingSpreadSpectrum(FHSS)**

* Frequency hopping is a spread spectrum technique thatinvolves transmitting the signal over a random sequence of frequencies.
* That is, first transmitting at one frequency, then a second, then a third, and so on.
* The random sequence of frequencies is computed by a pseudorandom number generator.
* Thereceiverusesthesamealgorithmasthesenderandinitializesitwiththe same seed and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.



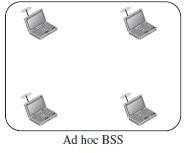
**DirectSequenceSpreadSpectrum(DSSS)**

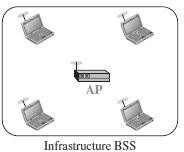
* Eachbitofdataisrepresentedbymultiplebitsinthetransmitted signal.
* DSSStakesauserdatastreamandperformsanXORoperationwitha pseudo –random number.
* Thispseudorandomnumberiscalledas***chippingsequence*.**



TOPOLOGYINWLAN/802.11

WLANscanbebuiltwitheitherofthefollowingtwotopologies/architecture:

* Infra-StructureNetworkTopology
* AdHocNetworkTopology



**Infra-Structure Topology**

**(APbasedTopology)**

* Anadhocnetworkisthearchitecture that is used to support mutual communication between wireless clients.
* Typically, an ad- hoc network is createdspontaneouslyanddoesnot support access to wired networks.
* Anadhocnetworkdoesnotrequire an AP.

**Ad-HocTopology**

**(Peer-to-Peer Topology)**

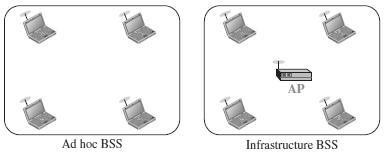
* An infrastructure network is the network architecture for providing communication between wireless clientsand wired networkresources.
* The transition of data from the wirelesstowiredmediumoccursvia a Base Station called AP(Access Point).
* An AP and its associated wireless clients define the coverage area.

ARCHITECUREOFWLAN/802.11

* Thestandarddefinestwokindsofservices:the BasicServiceSet(BSS)andthe Extended Service Set (ESS).

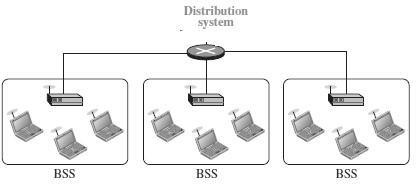
**BasicServiceSet(BSS)**

* IEEE802.11definesthe**basicserviceset(BSS)**asthebuildingblocksofa wireless LAN.
* Abasicservicesetismadeofstationaryormobilewirelessstationsandan optional central base station, known as the *access point (AP)*.



**ExtendedServiceSet(ESS)**

* Anextendedserviceset(ESS)is madeupoftwoormoreBSSswithAPs.
* Inthiscase,theBSSsareconnectedthrougha *distributionsystem,* whichisa wired or a wireless network.
* ThedistributionsystemconnectstheAPsintheBSSs.Theextendedserviceset uses two types of stations: mobile and stationary.
* ThemobilestationsarenormalstationsinsideaBSS.
* ThestationarystationsareAPstationsthatarepartofawiredLAN.



**StationTypes**

IEEE 802.11 defines three types of stationsbased on theirmobility in a wirelessLAN:

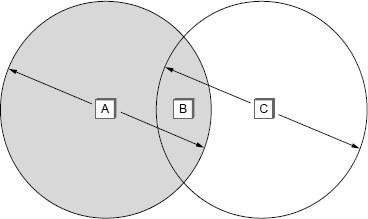
1. ***No-transition***-Astationwithno-transition mobilityiseitherstationary (not moving) or moving only inside a BSS.
2. ***BSS-transition*** -AstationwithBSS-transitionmobilitycanmovefrom one BSS to another, but the movement is confined inside one ESS

***ESS-transition*** - Astation with ESS-transition mobilitycan move fromone ESS to another.

COLLISIONAVOIDANCEINWLAN/802.11

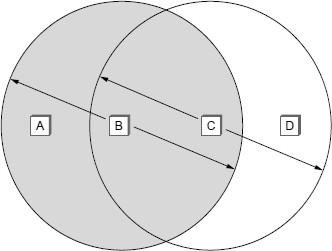
WirelessprotocolwouldfollowexactlythesamealgorithmastheEthernet—Wait until the link becomes idle before transmitting and back off should a collision occur.

**HiddenNodeProblem**

****

* + ConsiderthesituationshownintheFigure.
  + HereAandCarebothwithinrangeofBbutnotwitheachother.
  + SupposebothAand C wanttocommunicate withBandsotheyeachsenda frame to B.
  + AandCareunawareofeachothersincetheirsignalsdonotcarrythat far.
  + ThesetwoframescollidewitheachotheratB,butneitherAnorCisaware of this collision.
  + AandCaresaidtobe*hiddennodes*withrespecttoeachother.

**ExposedNodeProblem**

****

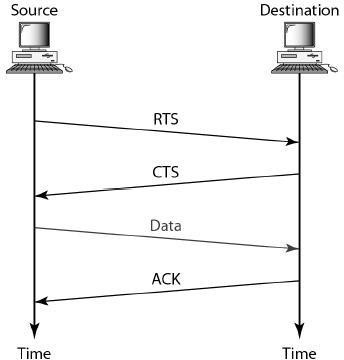
* + Each of the four nodes is able tosend and receive signals that reach just the nodes to its immediate left and right.
  + For example,B can exchange frames with A and C but it cannot reach D,while C can reach B and D but not A.
  + SupposeB issendingto A.Node C isaware of thiscommunication because it hears B’s transmission.
  + Ifatthesametime,CwantstotransmittonodeD.
  + It would be a mistake, however, for C to conclude that it cannot transmit to anyone just because it can hear B’s transmission.
  + Thisisnot aproblemsinceC’stransmissionto Dwillnotinterfere withA’s ability to receive from B.
  + Thisiscalledexposedproblem.
  + AlthoughBandCareexposedtoeachother’ssignals,thereisno interference if B transmits to A while C transmits to D.

MULTIPLEACCESSWITHCOLLISIONAVOIDANCE(MACA)

* MACA is used to avoid collisions caused by the hidden terminal problemand exposed terminal problem.
* MACAusesshort**signalingpackets**called**RTS**and**CTS**forcollision avoidance.
* The RTS and CTS signals helps us to determine who else is in the transmission range or who is busy.
* When a sender wants to transmit, it sends a signal called **Request-To-Send (RTS).**
* Ifthereceiverallowsthetransmission,itrepliestothesenderasignalcalled

Clear-To-Send(CTS).

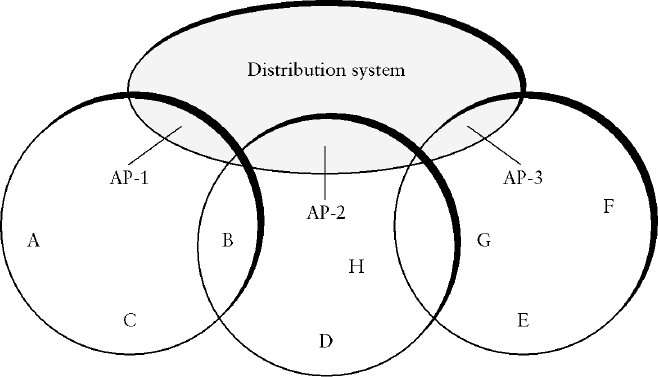
* Anynode that sees the CTSframe knows that it is closeto thereceiver, and therefore cannot transmit for the period of time.
* AnynodethatseestheRTSframebutnottheCTSframeisnotclose enough to the receiver to interfere with it, and so is free to transmit.
* TheSignalingpacketsRTSandCTScontainsinformationsuch as
  + senderaddress
  + receiveraddress
  + lengthofthedatatobesent/received



* ThereceiversendsanACKto thesenderaftersuccessfullyreceivinga frame.
* AllnodesmustwaitforthisACKbeforetryingtotransmit.
* WhentwoormorenodesdetectanidlelinkandtrytotransmitanRTSframeat the same time, their RTS frames will collide with each other.
* ***802.11 do not support collision detection,*** but instead, the senders realize the collision has happened when they do not receive the CTS frame after a period of time.
* Eachnodewaitsforarandomamountoftimebeforetryingagain.
* The amount of time a given node delays is defined by exponential back-off algorithm.

DISTRIBUTIONSYSTEMINWLAN/802.11

In wireless network, nodes can move freely. Some nodes are allowed to roam and some are connected to a wired network infrastructure called **access points (AP)**, and they are connected to each other by a so-called **distribution system**.



* + Two nodes can communicate directly with each other if they are within reach of each other,
  + When the nodes are at different range, for example when node A wish to communicate with node E, A first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E.

## ScanningProcessinDistributionSystem

* + The***techniqueforselectinganAccessPoint***iscalled***scanning.***
  + Scanningwilltakeplacewheneveranodejoinsthenetworkaswellas when it is not satisfied with the current access point signal.
  + Itinvolvesthefollowingfoursteps:
    - Thenodesendsa**ProbeRequest**frame.
    - AllAP’swithinreachreplywitha**ProbeResponse**frame.
    - ThenodeselectsoneoftheaccesspointsandsendsthatAPan

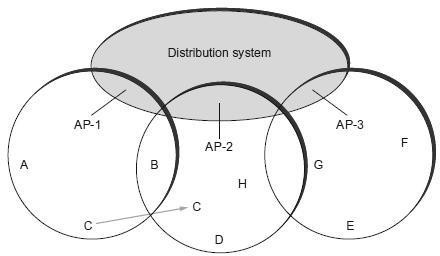
**AssociationRequest**frame.

* + - TheAPreplieswithan**AssociationResponse** frame.
  + TherearetwotypesofScanning.Theyare

1. ActiveScanning
2. PassiveScanning

***ActiveScanning***

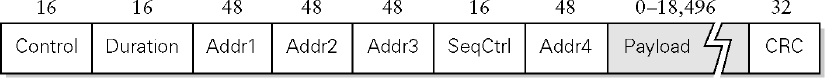
When node C moves from the cell serviced by AP-1 to the cell serviced by AP-2. As it moves, it sends Probe frames, which eventually result in Probe Response. Since the ***node is actively searching for an access point*** it is calledactive scanning.



***PassiveScanning***

***AP’s periodically send a Beacon frame to the nodes*** that advertisesthe capabilities of the access point which includes the transmission rates supported by the AP. This is called passive scanning and a node can change to this AP based on the Beacon frame simply by sending it an Association Request frame back to the access point.

FRAMEFORMATOFWLAN/802.11

****

* ***Controlfield***-containsthreesubfields:
* ***Typefield***-Indicates whethertheframecarriesdata,RTSorCTSframe
* ***ToDS***-DataframesenttoDS
* ***FromDS–***ACKsentfromDS

When both the DS bits are set to 0, it indicates that one node issending directly to another . Addr l identifies the target nodeand Addr2 identifies the source node.

When both the DS bits are set to 1, it indicates that one nodeissending the message to another indirectly using thedistribution system.

* ***Duration-***containsthedurationoftimethemediumisoccupiedbythenodes.
* ***Addr*l**-identifiesthefinaloriginaldestination
* ***Addr2***-identifiestheimmediatesender(theonethatforwardedtheframe from the distribution system to the ultimate destination)
* ***Addr 3*** - identifies the intermediate destination (the one that accepted the framefromawirelessnodeandforwardeditacrossthedistribution system)
  + ***Addr4*-**identifiestheoriginalsource
  + ***SequenceControl***-toavoidduplicationofframessequencenumber is

assignedtoeach frame

* + ***Payload*-**Datafromsendertoreceiver
  + ***CRC*-**usedforErrordetectionoftheframe.

## 10. BLUETOOTH(IEEE802.15.1)

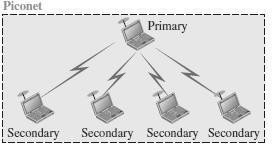
* + - A Bluetooth is an ad hoc network, which means that the network is formedspontaneously.
    - Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop),cameras,printers,whentheyareatashortdistancefromeachother.
    - Bluetoothtechnologyistheimplementationofaprotocoldefinedbythe IEEE 802.15 standard.
    - Thestandarddefinesawirelesspersonal-areanetwork(PAN)
    - Bluetoothoperatesinthe2.4GHzUnlicensedISMband.
    - TherangeforBluetoothcommunicationis0-30feet(10meters).
    - Thisdistancecanbeincreasedto100metersbyamplifyingthepower.
    - Bluetoothlinkshavetypicalbandwidthsaround1to3Mbps.
    - Bluetooth is specified by an industryconsortiumcalled the Bluetooth Special Interest Group.
    - UptoeightdevicescanbeconnectedthroughBluetooth.
    - One device will function as a Master and theother seven devices will function asslaves.
    - BluetoothusesFrequencyHoppingSpreadSpectrum(FHSS)toavoidany interference.
    - Bluetoothsupportstwokindsoflinks:
      * AsynchronousConnectionless(ACL)links-fordata
      * SynchronousConnectionoriented(SCO)links-foraudio/voice

### BLUETOOTHARCHITECTURE

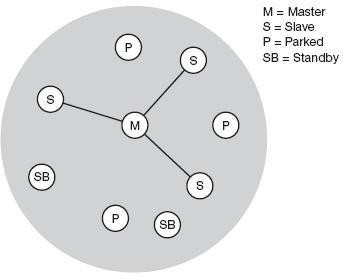
Bluetoothdefinestwotypesofnetworks:PiconetandScatternet.

PICONET

* ThebasicBluetoothnetworkconfigurationiscalledaPiconet
* APiconetisacollectionofeightbluetoothdeviceswhicharesynchronized.
* Onedeviceinthepiconetcanactas**Primary(M*aster*)**,allotherdevices connected to the master act as **Secondary (Slaves).**
* All thesecondary stations synchronizetheirclocks and hopping sequence with the primary.

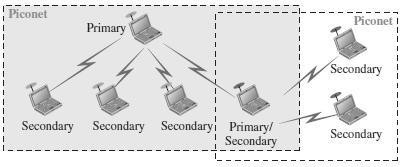


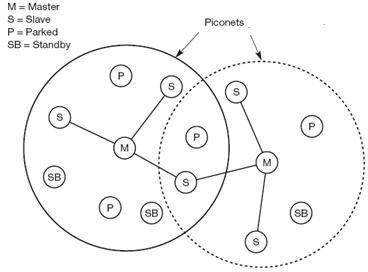
* Anycommunicationisbetweentheprimary/masterandasecondary/slave.
* Thecommunicationbetweentheprimaryandsecondarystationscanbe one-to-one or one-to-many.
* Theslavesdonotcommunicatedirectlywitheachother.
* Thedevicesinapiconetcanbeinanyoneofthethree types/states.
* Theyare
  + ActiveDevice/State
    1. Connectedtothepiconetandparticipatesinthecommunication.
    2. CanbeaMasteroraSlavedevice.
    3. Allactivedevicesareassigneda3-bitaddress(AMA).
  + ParkedDevice/State
    1. Connectedtothepiconet,butdoesnotactivelyarticipateinthe communication.
    2. Morethan200devicescanbeparked.
    3. Allparkeddevicesusean8-bitparkedmemberaddress(PMA).
  + Stand-byDevice/State
    1. Notconnectedtothepiconet.
    2. Theydonotparticipateinthepiconetcurrentlybutmaytakepartata later time.
    3. Devicesinstand-bydonotneedanaddress.



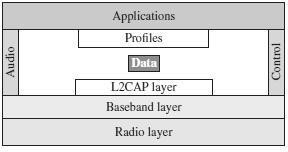
* If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park state to allow the parked device to switch to active state.

SCATTERNET

* + Piconetscanbecombinedtoformwhatiscalleda**scatternet.**
  + Manypiconetswithoverlappingcoveragecanexistsimultaneously,called Scatternet.
  + Asecondarystationinonepiconetcanbetheprimaryinanotherpiconet.
  + This station can receive messages from the primary in the first piconet (as a secondary)and, actingasaprimary, deliverthemtosecondariesinthesecond piconet.
  + Astationcanbeamemberoftwopiconets.
  + Intheexamplegivenbelow,therearetwopiconets,inwhichoneslaveparticipates in two different piconets.
  + Masterofonepiconetcannotactasthemasterofanotherpiconet.
  + ButtheMasterofonepiconetcanactasaSlaveinanotherpiconet



BLUETOOTHLAYERS

****

RadioLayer

* + - The radio layer is roughly equivalent to the physical layer of the Internet model.
    - Bluetooth uses the **frequency-hopping spread spectrum (FHSS)** method in the physical layer to avoid interference from other devices or other networks.
    - Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.
    - Totransformbitstoasignal,Bluetoothusesa sophisticated versionofFSK, called GFSK.

BasebandLayer

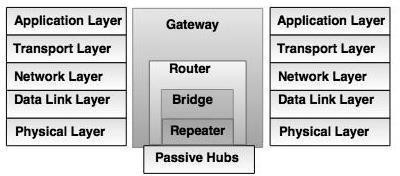
* + - ThebasebandlayerisroughlyequivalenttotheMACsublayerinLANs.
    - TheaccessmethodisTDMA.
    - Theprimaryandsecondarystationscommunicatewitheachotherusing time slots. The length of a time slot is exactly 625 µs.
    - During thattime, a primary sends a frame to a secondary, or a secondarysends a frame to the primary.

L2CAP

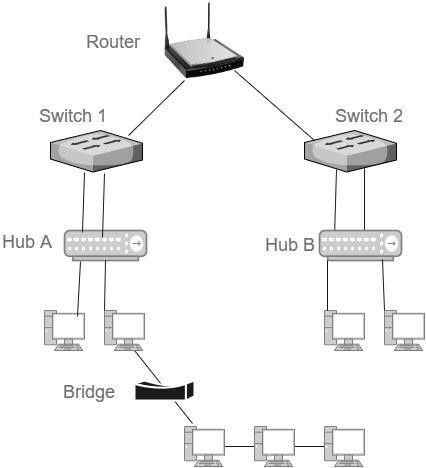
* + - The **Logical Link Control and Adaptation Protocol,** or **L2CAP** (L2 here means LL) is equivalent to the LLC sublayer in LANs.
    - ItisusedfordataexchangeonanACLlink.
    - SCOchannelsdonotuseL2CAP.
    - TheL2CAPfunctionsare :multiplexing,segmentationandreassembly, quality of service (QoS), and group management.

**11. CONNECTINGDEVICES**

* + - Connectingdevices are used toconnecthoststogetherto make anetworkor to connect networks together to make an internet.
    - ConnectingdevicescanoperateindifferentlayersoftheInternetmodel.

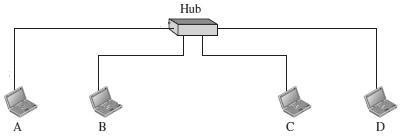


* + - Connectingdevices are divided into five different categories on the basis of layers in which they operate in the network.



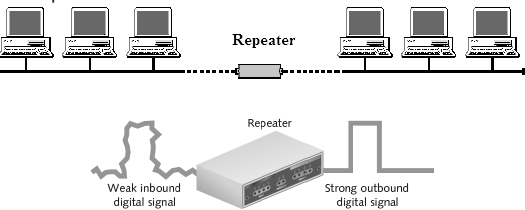
1. Deviceswhichoperatebelowthephysicallayer -**Passivehub**.
2. Deviceswhichoperateatthephysicallayer-**Repeater**.
3. Deviceswhichoperateatthephysicalanddatalinklayers-**Bridge**.
4. Deviceswhichoperateatthephysicallayer,datalinklayerandnetworklayer–

Router.

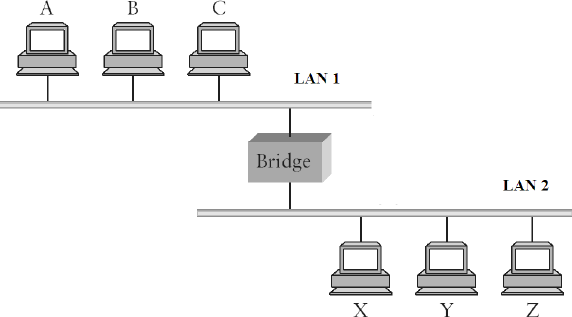
1. Deviceswhichoperateatallfivelayers-**Gateway**.
2. HUBS
   * Several networks need a central location to connect media segments together. These central locations are called as hubs.
   * The hub organizes the cables and transmits incoming signals to the other media segments.

Thethreetypesofhubsare:

1. **Passivehub**
   * Itisaconnector,whichconnectswirescomingfromthedifferentbranches.
   * By using passive hub, each computer can receive the signal which is sentfrom all other computers connected in the hub.
2. ActiveHub
   * Itisamultiportrepeater,whichcanregeneratethesignal.
   * It is used to create connections between two or more stations in a physical star topology.
3. IntelligentHub
   * Intelligent hub contains a program of network management and intelligent path selection.
4. REPEATERS
   * A repeaterreceivesthesignaland itregeneratesthesignalinoriginalbit pattern before the signal gets too weak or corrupted.
   * ItisusedtoextendthephysicaldistanceofLAN.
   * Repeaterworksonphysicallayer.
   * Arepeaterhasnofilteringcapability**.**
   * A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes.
   * Repeaters amplify thereceived/input signal to a higher frequency domain so that it is reusable, scalable and available.
   * Repeatersarealsoknownas**signalboosters**or**rangeextender.**
   * A repeater cannot connect two LANs, but it connects two segments of the same LAN.



1. BRIDGES
   * Bridgesoperateinphysicallayeraswellasdatalinklayer.
   * Asaphysicallayerdevice,theyregeneratethereceivesignal.
   * As a data link layer, the bridge checks the physical (MAC) address (of the source and the destination) contained in the frame.
   * Thebridgehasafilteringfeature.
   * It cancheck thedestinationaddressof a frameanddecides,if theframe should be forwarded or dropped.
   * BridgesareusedtoconnecttwoorLANs workingonthesameprotocol.



TypesofBridges:

* **TransparentBridges**

These are the bridge in which the stations are completely unaware 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.

* SourceRoutingBridges

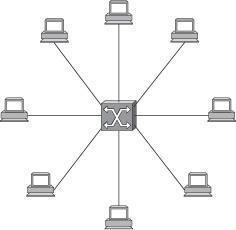
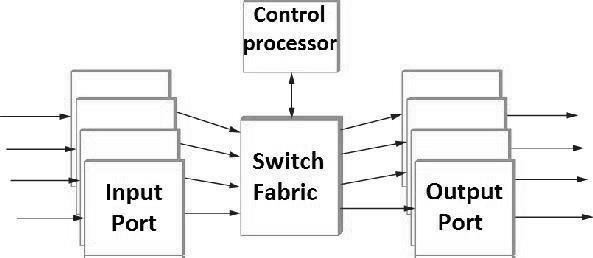
In these bridges, routing operation is performed by source station and theframe specifies which route to follow.

* TranslationBridges

These bridges connect networks with different architectures, such as Ethernetand Token Ring. These bridges appear as:

* + TransparentbridgestoanEthernethost
  + Source-routingbridgestoaTokenRinghost

1. SWITCHES

* A switch is a small hardwaredevice which is used to join multiplecomputers together with one local area network (LAN).
* A switch is a mechanism that allows us to interconnect links to form a large network.
* Switchisdatalinklayerdevice.
* Aswitchisamultiportbridgewithabuffer.
* SwitchesareusedtoforwardthepacketsbasedonMACaddresses.
* Itisoperatedinfullduplexmode.
* Packetcollisionisminimumasitdirectlycommunicatesbetweensource and destination.
* Itdoesnotbroadcastthemessageasitworkswithlimitedbandwidth.
* A switch’sprimary jobistoreceiveincoming packetsononeofitslinks and to transmit them on some other link.
* ASwitchisusedtotransferthedataonlytothedevicethathasbeenaddressed.

51

* Input ports receive stream of packets, analyzes the header, determines theoutput port and passes the packet onto the fabric.
* Portscontainbufferstoholdpacketsbeforeitisforwarded.
* Ifbufferspaceisunavailable,thenpacketsaredropped.
* Ifpacketsatseveralinputportsqueueforasingleoutputport,thenonlyone of them is forwarded.

TypesofSwitch

1. **Two-LayerSwitch**
   * Thetwo-layerswitchperformsatthephysicalandthedatalinklayer.
   * Itisabridgewithmanyportsanddesignallowsfasterperforms.
   * AbridgeisusedtoconnectdifferentLANstogether.
   * The two- layer switch can make a filtering decision bases on the MAC address of the received frame. However, two- layer switch has a buffer which holds the frame for processing.
2. Three-LayerSwitch
   * Thethree-layerswitchisarouter.
   * Theswitchingfabric inathree-layer allowsafastertablelookupand forwarding mechanism.
3. ROUTERS

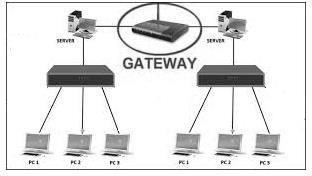
* Arouterisathree-layerdevice.
* Itoperatesinthephysical,data-link,andnetworklayers.
* Asaphysical-layerdevice,itregeneratesthesignalitreceives.
* As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet.
* Asanetwork-layerdevice,arouterchecksthenetwork-layeraddresses.
* A router is a device like a switch that routes data packets based on their IP addresses.
* Arouter can connect networks. Arouter connects the LANs and WANs on the internet.
* Arouterisaninternetworkingdevice.
* Itconnectsindependentnetworkstoformaninternetwork.



* The key function of the router is to determine the shortest path to the destination.
* Router has a routing table, which is used to make decision on selecting the route.
* The routing table is updated dynamically based on which they make decisions on routing the data packets.

1. GATEWAY

* A gateway is a device,which operates inall five layersofthe internet orseven layers of OSI model.
* Itisusuallyacombinationofhardwareandsoftware.
* Gatewayconnectstwoindependentnetworks.



* Gatewaysaregenerallymorecomplexthanswitchorrouter.
* Gateways basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
* Gatewaysarealsocalledprotocolconverters
* A gateway accepts a packet formatted for one protocol and converts it to a packet formatted to another protocol before forwarding it.
* Thegatewaymustadjustthedatarate,sizeanddataformat.

1. BROUTER

* Brouterisahybriddevice.Itcombinesthefeaturesofbothbridgeand router.
* BrouterisacombinationofBridgeandRouter.
* Functionsasabridgefornonroutableprotocolsandarouterforroutable protocols.
* Asarouter,itiscapableofroutingpacketsacross networks.
* Asabridge,itiscapableoffilteringlocalareanetworktraffic.
* Providesthebestattributesofbothabridgeandarouter
* Operatesat both theData Linkand Networklayers and canreplace separate bridges and routers.

**UNITIII-NETWORKLAYER**

**Network Layer Services – Packet Switching – Performance – IPV4 Addresses–ForwardingofIPPackets –NetworkLayerProtocols:IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics** – **IPV6 Addressing – IPV6 Protocol**

**1. NETWORKLAYERSERVICES**

* The network layer in the TCP/IP protocol suite is responsible for the host-to-host delivery of datagrams.
* It provides services to the transport layer and receives services from the data-link layer.
* Thenetworklayertranslatesthelogicaladdressesintophysicaladdresses
* It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
* The main role of the networklayer is to move the packets fromsendinghost to the receiving host.

#### Servicesprovidedbynetworklayerare

PACKETIZING

* Thefirstdutyofthenetworklayerisdefinitely packetizing.
* This means encapsulating the payload (data received from upper layer) in a network-layerpacketatthesourceanddecapsulatingthepayloadfromthe network-layer packet at the destination.
* Thenetwork layerisresponsiblefor deliveryof packets from a sender toa receiver without changing or using the contents.

**ROUTINGANDFORWARDING**

#### Routing

* The network layer is responsible for routing the packet from its source to thedestination.
* The network layer is responsible for finding the best one among these possible routes.
* The network layer needs to have some specific strategies for defining the best route.
* Routing is the concept of applying strategies and running routing protocols to create the decision-making tables for each router.
* Thesetablesarecalledasroutingtables.

#### Forwarding

* Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.
* The decision-making table,a routernormallyusesfor applying thisaction is called the forwarding table.
* When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.

ERRORCONTROL

* ThenetworklayerintheInternetdoesnotdirectlyprovideerrorcontrol.
* It addsachecksumfieldtothedatagramtocontrolanycorruptioninthe header, but not in the whole datagram.
* This checksum prevents any changes or corruptions in the header of the datagram.
* TheInternetusesanauxiliaryprotocolcalledICMP,thatprovidessomekind of error control if the datagram is discarded or has some unknown information in the header.

FLOWCONTROL

* Flowcontrolregulatestheamountofdataasourcecansendwithout overwhelming the receiver.
* The network layer in the Internet, however, does not directly provide any flow control.
* The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.
* Flowcontrolisprovidedformostoftheupper-layerprotocolsthatusethe servicesofthenetworklayer, soanotherlevel offlowcontrolmakes the network layer more complicated and the whole system less efficient.

CONGESTIONCONTROL

* Anotherissueinanetwork-layerprotocoliscongestioncontrol.
* Congestion in the networklayer is asituation in which too many datagrams are present in an area of the Internet.
* Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.
* Inthissituation,someroutersmaydropsomeofthedatagrams.

SECURITY

* Anotherissuerelatedtocommunicationatthenetworklayerissecurity.
* To provide security for a connectionless network layer,weneedtohave another virtuallevelthatchangesthe connectionlessservicetoaconnection- oriented service. This virtual layer is called ascalled IPSec (IP Security).

**2. PACKETSWITCHING**

(REFERTHETOPICPACKETSWITCHINGFROMUNIT–I)

**3. NETWORK-LAYERPERFORMANCE**

* Theperformanceofanetworkcanbemeasuredinterms of

Delay,ThroughputandPacketloss.

* Congestioncontrolisanissuethatcanimprovetheperformance.

### DELAY

* Apacketfromitssourcetoitsdestination,encountersdelays.
* Thedelaysinanetworkcanbedividedintofourtypes:

Transmissiondelay,Propagationdelay,ProcessingdelayandQueuingdelay.

#### TransmissionDelay

* Asourcehostoraroutercannotsendapacketinstantaneously.
* Asenderneedstoputthebitsinapacketonthelineonebyone.
* Ifthe first bit of the packet is put on the line at time t 1andthelastbitisputon the line at time t2, transmission delay of the packet is (t2 - t1).
* The transmission delay is longer for a longer packet and shorter if the sendercan transmit faster.
* TheTransmissiondelayiscalculatedusingthe formula

Delaytr=(Packetlength)/(Transmissionrate)

* Example:

InaFastEthernet LANwiththetransmissionrateof100millionbitsper second and a packet of 10,000 bits, it takes (10,000)/(100,000,000) or 100 microseconds for all bits of the packet to be put on the line.

#### PropagationDelay

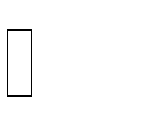
* Propagation delay is the time it takes for a bit to travel frompoint Ato point B in the transmission media.
* Thepropagationdelayforapacket-switchednetworkdependsonthe propagation delay of each network (LAN or WAN).
* Thepropagationdelaydependsonthepropagationspeedofthemedia,whichis

3X108meters/secondinavacuumandnormallymuchlessinawiredmedium.

* Italsodependsonthedistanceofthelink.
* ThePropagationdelayiscalculatedusingtheformula

Delaypg=(Distance)/(Propagationspeed)

* Example

If the distance of a cable link in a point-to-point WAN is 2000 meters and thepropagationspeedofthebitsin thecable is 2X108 meters/second,then the propagation delay is 10 microseconds.

#### ProcessingDelay

* The processing delay is the time required for a router or a destination host to receiveapacketfromitsinputport,removetheheader,performanerrordetectionprocedure,and deliverthepackettotheoutputport(in the caseofa

router)ordeliverthepackettotheupper-layerprotocol(inthecaseofthe destination host).

* The processing delay may be different for each packet, but normally is calculated as an average.

**Delaypr**=**Timerequiredtoprocessapacketinarouteroradestinationhost**

#### QueuingDelay

* Queuingdelaycannormallyhappeninarouter.
* Arouterhasaninputqueueconnectedtoeach ofitsinputportstostorepackets waiting to be processed.
* Therouteralsohasanoutputqueueconnectedtoeachofitsoutputportsto store packets waiting to be transmitted.
* Thequeuingdelayforapacketinarouterismeasuredasthetimeapacket waits in the input queue and output queue of a router.

**Delayqu**=**Thetimeapacket waitsininputandoutputqueuesinarouter**

#### TotalDelay

* Assuming equal delays for the sender, routers and receiver, the total delay (source-to-destinationdelay)ofapacketcanbecalculatedifweknowthe number of routers, n, in the whole path.

Totaldelay=(n+1)(Delaytr+Delaypg+Delaypr)+(n)(Delayqu)

* Ifwehavenrouters,wehave(n**+**1)links.
* Therefore, we have (n **+**1) transmission delays related to n routersandthe source,(n **+**1)propagationdelaysrelatedto(n **+**1) links, (n **+**1) processing delaysrelatedtonroutersandthedestination,andonlynqueuingdelaysrelated to n routers.

### THROUGHPUT

* Throughput at any point in a network is defined as the number of bits passingthrough the point in a second, which is actually the transmission rate of data at that point.
* In a path from sourceto destination,a packetmay pass through several links(networks), each with a different transmission rate.
* Throughputiscalculatedusingtheformula

Throughput=minimum{TR1,TR2,...TRn}

* Example:

Let us assume that we have three links, each with a different transmissionrate.

The data can flow at the rate of 200 kbps in Link1, 100 kbps in Link2 and150kbps in Link3.

Throughput=minimum{200,100,150}=100.

### PACKETLOSS

* Anotherissuethatseverelyaffectstheperformanceofcommunicationisthe number of packets lost during transmission.
* When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
* Arouterhasaninputbufferwithalimitedsize.
* Atimemaycomewhenthebufferisfullandthenextpacketneedstobe dropped.
* The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.

### CONGESTIONCONTROL

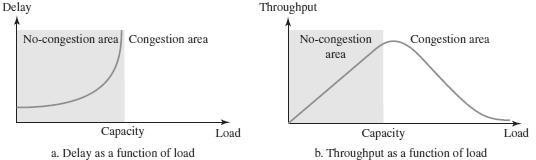
* Congestionatthenetworklayerisrelatedtotwoissues,throughputanddelay.

BasedonDelay

* When the load is much less than the capacity of the network, the delay is at aminimum.
* This minimum delay is composed of propagation delay and processing delay,both of which are negligible.
* However,whentheloadreachesthenetworkcapacity,thedelayincreases sharply because we now need to add the queuing delay to the total delay.
* Thedelaybecomesinfinitewhentheloadisgreaterthanthecapacity.

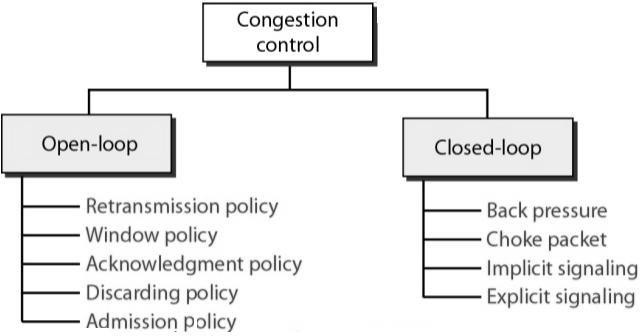
BasedonThroughout

* When the load is below the capacity of the network, the throughput increasesproportionally with the load.
* We expect the throughput to remain constant after the load reaches thecapacity, but instead the throughput declines sharply.
* Thereasonisthediscardingofpacketsbytherouters.
* Whentheloadexceedsthecapacity,thequeuesbecomefullandtherouters have to discard some packets.
* Discarding packets does not reduce the number of packets inthenetwork because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destinations.



#### CongestionControlMechanisms

* Congestioncontrolisamechanismforimprovingperformance.
* Itreferstotechniques andmechanismsthatcaneitherpreventcongestion before it happens or remove congestion after it has happened.
* In general, we can divide congestion control mechanisms into two broad categories:
  + **Open-loopCongestioncontrol**(prevention)
  + **Closed-loopCongestioncontrol**(removal)



**OPEN-LOOPCONGESTIONCONTROL**

* Inopen-loopcongestioncontrol,policiesareappliedtopreventcongestion before it happens.
* In these mechanisms, congestion control is handled by either the source or the destination.

RetransmissionPolicy

* + Retransmissionissometimesunavoidable.
  + Ifthesenderfeelsthatasentpacketislostorcorrupted,thepacket needs to be retransmitted.
  + Retransmissioningeneralmayincreasecongestioninthenetwork.
  + However,agoodretransmissionpolicycanpreventcongestion.
  + Theretransmissionpolicyandtheretransmissiontimersmustbe designedtooptimizeefficiencyandatthesametimepreventcongestion.

WindowPolicy

* + Thetypeofwindowatthesendermayalsoaffectcongestion.
  + The Selective Repeat window is better than the Go-Back-N window for congestion control.
  + In the Go-Back-N window, when the timer for apackettimesout, severalpackets may beresent, although some may have arrivedsafe and sound at the receiver.
  + Thisduplicationmaymakethecongestionworse.
  + The Selective Repeat window, ontheother hand, triesto sendthe specific packets that have been lost or corrupted.

AcknowledgmentPolicy

* + Theacknowledgmentpolicyimposedbythereceivermayalsoaffect congestion.
  + Ifthereceiverdoesnotacknowledgeeverypacketitreceives,itmay slow down the sender and help prevent congestion.
  + Severalapproachesareusedinthiscase.
  + A receivermaysendanacknowledgmentonlyifithasapackettobe sent or a special timer expires.
  + AreceivermaydecidetoacknowledgeonlyNpacketsatatime.
  + Sending fewer acknowledgments means imposing less load on the network.

DiscardingPolicy

* + A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
  + For example, in audio transmission, if the policy is to discard less sensitivepacketswhencongestionislikelytohappen,thequalityof sound is still preserved and congestion is prevented or alleviated.

AdmissionPolicy

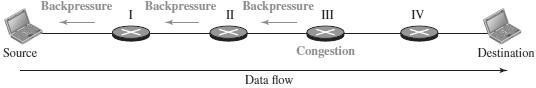
* + An admission policy, which is a quality-of-service mechanism can also prevent congestion in virtual-circuit networks.
  + Switches in a flow first check the resource requirement of a flow before admitting it to the network.
  + Aroutercandenyestablishingavirtual-circuitconnectionifthereis congestioninthenetworkorifthereisapossibilityoffuturecongestion.

**CLOSED-LOOPCONGESTIONCONTROL**

* Closed-loop congestion control mechanisms try to alleviate congestion after it happens.
* Severalmechanismshavebeenusedbydifferentprotocols.

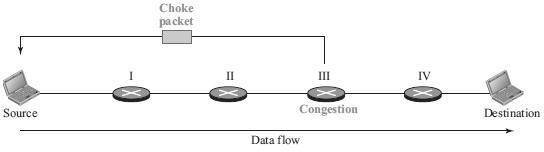
Backpressure

* + The technique of backpressure refers to a congestion control mechanism inwhichacongestednodestopsreceivingdatafromtheimmediate upstream node or nodes.
  + This may cause the upstream node or nodes to become congested, andthey, in turn, reject data from their upstream node or nodes, and so on.
  + Backpressureisanode-to-nodecongestioncontrolthatstartswitha node and propagates, in the opposite direction of data flow, to the source.
  + The backpressure technique can be applied only to virtual circuitnetworks, in which each node knows the upstream node from which aflow of data is coming.



ChokePacket

* + A choke packet is a packet sent by a node to the source to inform it ofcongestion.
  + Inbackpressure,thewarningisfromonenodetoitsupstreamnode, although the warning may eventually reach the source station.
  + In the choke-packet method, the warning is from the router, which hasencountered congestion, directly to the source station.
  + Theintermediatenodesthroughwhichthepackethastraveledarenot warned.
  + The warning message goes directly to the source station; the intermediate routers do not take any action.



Implicit Signaling

* + In implicit signaling, there is no communication between the congested node or nodes and the source.
  + The source guesses that there is congestion somewhere in the networkfrom other symptoms.
  + For example, when a source sends several packets and there is no acknowledgmentforawhile,oneassumptionisthatthenetworkis congested.
  + The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

ExplicitSignaling

* + The node that experiences congestion can explicitly send a signal to the source or destination.
  + Theexplicit-signalingmethodisdifferentfromthechoke-packet method.
  + Inthechoke-packetmethod,aseparatepacketisusedforthispurpose; intheexplicit-signalingmethod,thesignalisincludedinthepackets that carry data.
  + Explicit signaling can occur in either the forward or the backward direction.

## 4.IPV4 ADDRESSES

* The identifier used in the IP layer of the TCP/IP protocol suite to identify theconnectionofeachdevicetotheInternetiscalledtheInternetaddressorIP address.
* InternetProtocolversion4(IPv4)isthefourthversioninthedevelopmentof theInternetProtocol(IP)andthefirstversionoftheprotocoltobewidely deployed.
* IPv4isdescribedinIETFpublicationinSeptember1981.
* The IP address is the address of the connection, not the host or the router. AnIPv4 address is a 32-bit address that uniquely and universally defines the connection .
* Ifthedeviceis movedtoanothernetwork, theIPaddressmaybechanged.
* IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet.
* IfadevicehastwoconnectionstotheInternet,viatwonetworks,ithastwo IPv4 addresses.
* Pv4addressesareuniversalinthesensethattheaddressingsystemmustbe accepted by any host that wants to be connected to the Internet.

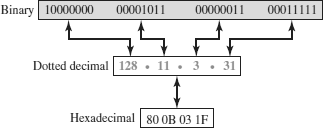
IPV4ADDRESSSPACE

* IPv4definesaddresseshasanaddressspace.
* Anaddressspaceisthetotalnumberofaddressesusedbytheprotocol.
* If a protocol uses *b* bits to define an address, the address space is 2 *b*because each bit can have two different values (0 or 1).
* IPv4uses32-bitaddresses,whichmeansthattheaddressspaceis2 32or 4,294,967,296 (more than four billion).
* 4billiondevicescouldbeconnectedtothe Internet.

IPV4ADDRESSNOTATION

TherearethreecommonnotationstoshowanIPv4address:

1. binarynotation(base 2), (ii)dotted-decimalnotation(base256),and
2. hexadecimalnotation(base16).



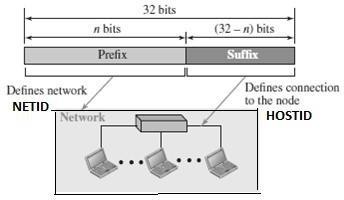
In*binary notation,*an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces are usually inserted between bytes (8 bits).

In *dotted-decimal notation,IPv4 addresses are* usually written in decimal form with a decimal point (dot) separating the bytes.Each number in the dotted-decimal notation is between 0 and 255.

In hexadecimal notation, each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits. This notation is often used in network programming.

HIERARCHYINIPV4ADDRESSING

* In any communication networkthat involves delivery, the addressingsystemis hierarchical.
* A32-bitIPv4addressisalsohierarchical,butdividedonlyintotwoparts.
* The first part of the address, called the*prefix*,defines the network(Net ID); the second part of the address, called the *suffix*, defines the node (Host ID).
* Theprefixlengthis*n*bitsandthesuffixlengthis(32- *n*)bits.



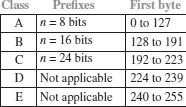
* Aprefixcanbefixedlengthorvariablelength.
* ThenetworkidentifierintheIPv4wasfirstdesignedasafixed-lengthprefix.
* Thisschemeisreferredtoasclassfuladdressing.
* The new scheme, which is referred to as classless addressing, uses a variable- length network prefix.

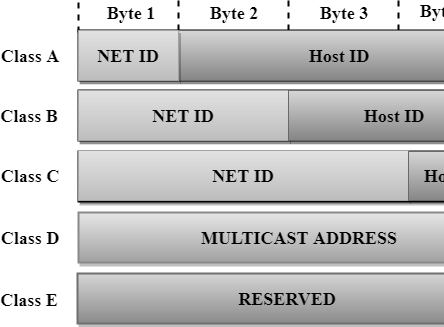
CATEGORIESOFIPV4ADDRESSING

* TherearetwobroadcategoriesofIPv4Addressingtechniques.
* Theyare
  + ClassfulAddressing
  + ClasslessAddressing

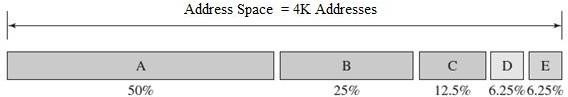
CLASSFULADDRESSING

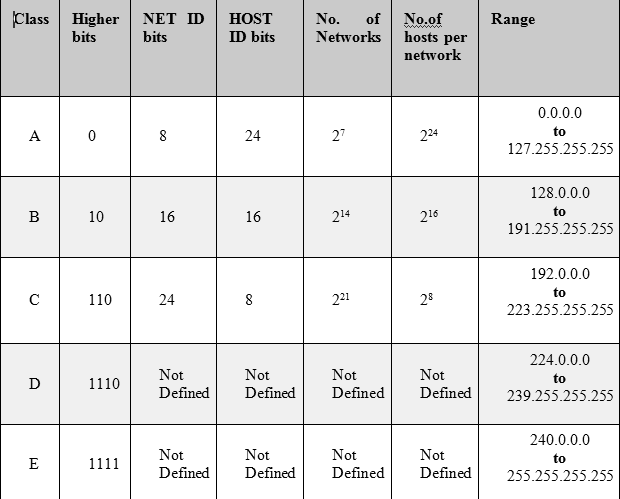
* AnIPv4addressis32-bitlong(4bytes).
* AnIPv4addressisdividedintosub-classes:





#### ClassfulNetworkArchitecture

****



**ClassA**

* InClassA,anIPaddressisassignedtothosenetworksthatcontainalarge number of hosts.
* ThenetworkIDis8bitslong.
* ThehostIDis24bitslong.
* In Class A,the first bit in higherorder bits of the first octet is always set to 0and the remaining 7 bits determine the network ID.
* The24bitsdeterminethehostIDinanynetwork.
* ThetotalnumberofnetworksinClassA=2 7=128networkaddress
* ThetotalnumberofhostsinClassA=2 24-2=16,777,214host address

#### ClassB

* In Class B, an IP address is assigned to those networks that range from small- sized to large-sized networks.
* TheNetworkIDis16bitslong.
* TheHostIDis16bitslong.
* InClassB,thehigherorderbitsofthefirstoctetisalwayssetto10,andthe remaining14 bits determine the network ID.
* Theother16bitsdeterminetheHostID.
* ThetotalnumberofnetworksinClassB=2 14=16384networkaddress
* Thetotalnumberofhostsin ClassB=2 16-2=65534hostaddress



#### ClassC

* InClassC,anIPaddressisassignedtoonlysmall-sizednetworks.
* TheNetworkIDis24bitslong.
* ThehostIDis8bits long.
* In Class C, the higher order bits of the first octet is always set to 110, and theremaining 21 bits determine the network ID.
* The8bitsofthehostID determinethehostina network.
* Thetotalnumberofnetworks=2 21=2097152networkaddress
* Thetotalnumberofhosts=2 8- 2=254hostaddress



#### ClassD

* InClassD,anIPaddressisreservedformulticast addresses.
* Itdoesnotpossesssubnetting.
* The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



#### ClassE

* InClassE,anIPaddressisusedforthefutureuseorfortheresearchand development purposes.
* Itdoesnotpossessanysubnetting.
* The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



#### AddressDepletioninClassfulAddressing

* Thereasonthatclassfuladdressinghasbecomeobsoleteisaddressdepletion.
* Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up.
* Thisresults in no more addresses available for organizations and individuals that needed to be connected to the Internet.
* Tounderstandtheproblem,letusthinkaboutclass A.
* Thisclasscanbeassignedtoonly128organizationsintheworld,buteach organization needs to have a single network with 16,777,216 nodes .
* Sincetheremaybeonlyafeworganizationsthatarethislarge,mostofthe addresses in this class were wasted (unused).
* ClassBaddressesweredesignedformidsizeorganizations,butmanyofthe addresses in this class also remained unused.
* Class C addresses have a completely different flaw in design. The number ofaddressesthatcanbeusedineachnetwork(256)wassosmallthatmostcompanies were not comfortable using a block in this address class.
* ClassEaddresseswerealmostneverused,wastingthewholeclass.

#### AdvantageofClassfulAddressing

* Although classful addressinghad several problems and became obsolete, it had one advantage.
* Givenanaddress,wecaneasilyfindtheclassoftheaddressand,sincethe prefixlengthforeachclassisfixed,wecanfindtheprefixlengthimmediately.
* In other words, the prefix length in classful addressing is inherent in the address;noextrainformationisneededtoextracttheprefixandthesuffix.

#### SubnettingandSupernetting

* Toalleviateaddressdepletion,twostrategieswereproposedandimplemented:

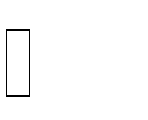
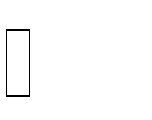
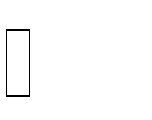
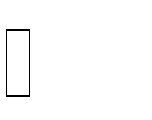
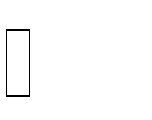
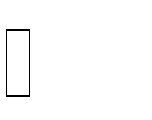
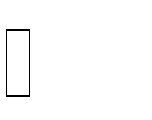
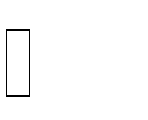
(i)Subnetting and (ii)Supernetting.

##### Subnetting

* Insubnetting,aclassAorclassBblockisdividedintoseveralsubnets.
* Eachsubnethasalargerprefixlengththantheoriginalnetwork.
* For example, if a network in class A is divided into four subnets, each subnethas a prefix of nsub= 10.
* At the same time, if all of the addresses in a network are not used, subnettingallows the addresses to be divided among several organizations.

CLASSLESSADDRESSING

* In 1996, the Internet authorities announced a new architecture called**classless addressing.**
* In classless addressing, variable-length blocks are used that belong to no classes.
* We can have a blockof 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.
* In classless addressing, the whole address space is divided into variable length blocks.
* Theprefixinanaddressdefinestheblock(network);thesuffixdefinesthe node (device).
* Theoretically,wecanhaveablockof2 0,21,22, 232addresses.



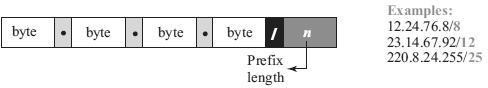
* The number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses.



* Theprefixlengthinclasslessaddressingisvariable.
* Wecanhaveaprefixlengththatrangesfrom0to 32.
* Thesizeofthenetworkisinverselyproportionaltothelengthoftheprefix.
* Asmallprefixmeansalargernetwork;alargeprefixmeansasmallernetwork.
* Theideaofclasslessaddressingcanbeeasilyappliedtoclassfuladdressing.
* AnaddressinclassAcanbethoughtofasaclasslessaddressinwhichthe prefix length is 8.
* AnaddressinclassBcanbethoughtofasaclasslessaddressinwhichthe prefix is 16, and so on. In other words, classful addressing is a special case of classless addressing.

#### NotationusedinClasslessAddressing

* Thenotationused inclasslessaddressingisinformallyreferredtoas*slash notation* and formally as ***classless interdomain routing*** or ***CIDR.***

******

* Forexample,192.168.100.14**/24**representstheIPaddress192.168.100.14 and, its subnet mask 255.255.255.0, which has 24 leading 1-bits.

#### AddressAggregation

* OneoftheadvantagesoftheCIDRstrategyis**addressaggregation**

(sometimescalled*addresssummarization*or*routesummarization*).

* When blocks of addresses are combined to create a larger block, routingcan be done based on the prefix of the larger block.
* ICANNassignsalargeblockofaddressestoanISP.
* Each ISP in turn divides its assigned block into smaller subblocks and grantsthe subblocks to its customers.

#### SpecialAddressesinIPv4

* There are five special addresses that are used for special purposes: *this-host* address, *limited-broadcast*address, *loopback*address, *private* addresses, and *multicast* addresses.

This-hostAddress

* Theonlyaddressintheblock**0.0.0.0**/**32**iscalledthe*this-host*address.
* ItisusedwheneverahostneedstosendanIPdatagrambutitdoesnotknowits own address to use as the source address.

Limited-broadcastAddress

* The only address in the block**255.255.255.255**/**32**is called the*limited- broadcast* address.
* It is used whenever a router orahost needs tosend a datagramto all devices in a network.
* The routers in the network,however,block the packet having this address asthe destination;the packet cannot travel outside the network.

LoopbackAddress

* Theblock**127.0.0.0**/**8**iscalledthe*loopback*address.
* Apacketwithoneoftheaddressesinthisblockasthedestinationaddress never leaves the host; it will remain in the host.

PrivateAddresses

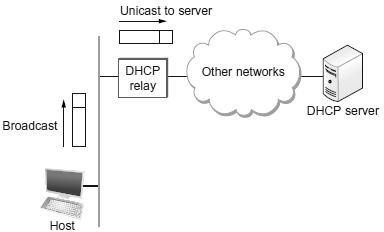
* Fourblocksareassignedasprivateaddresses:10.0.0.0/**8**,172.16.0.0/**12**, 192.168.0.0/**16**, and 169.254.0.0/**16**.

MulticastAddresses

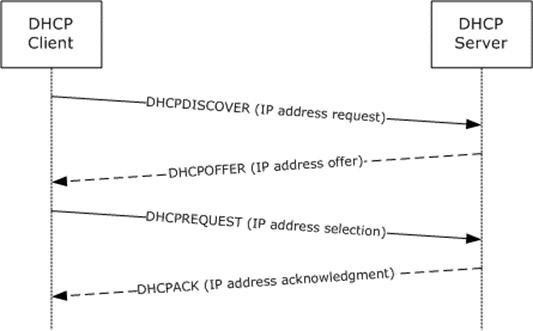
* Theblock224.0.0.0/**4**isreservedformulticast addresses.

**5. DHCP–DYNAMICHOSTCONFIGURATIONPROTOCOL**

* The dynamic host configuration protocol is used to simplify the installation andmaintenance of networked computers.
* DHCPisderivedfromanearlierprotocolcalledBOOTP.
* Ethernetaddressesareconfiguredintonetworkbymanufacturerandtheyare unique.
* IPaddressesmustbeuniqueonagiveninternetworkbutalsomustreflectthe structure of the internetwork
* Most host Operating Systems provide a way to manually configure the IP information for the host
* Drawbacksofmanualconfiguration:
  1. Alotofworktoconfigureallthehostsinalargenetwork
  2. Configurationprocessiserror-prune
* It is necessary to ensure that every host gets the correct network number and thatno two hosts receive the same IP address.
* Forthesereasons,automatedconfigurationmethodsarerequired.
* Theprimarymethodusesaprotocolknownasthe*DynamicHost Configuration Protocol* (DHCP).
* ThemaingoalofDHCPistominimizetheamountofmanualconfigurationrequired for a host.
* Ifanewcomputerisconnectedtoanetwork,DHCPcanprovideitwithallthe necessary information for full system integration into the network.
* DHCPisbasedonaclient/servermodel.
* DHCP clients send a request to a DHCP server to which the server responds with an IP address
* DHCPserverisresponsibleforprovidingconfigurationinformationtohosts.
* ThereisatleastoneDHCPserverforanadministrativedomain.
* TheDHCPservercanfunctionjustasacentralizedrepositoryforhost configuration information.
* The DHCP server maintains a pool of available addresses that it hands outto hosts on demand.

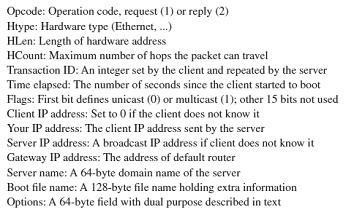
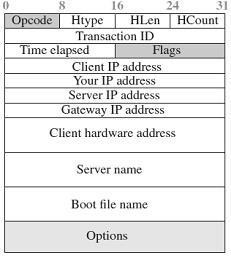


* Anewly bootedorattachedhostsendsaDHCPDISCOVER message toaspecial IP address (255.255.255.255., which is an IP broadcast address.
* Thismeansitwillbereceivedbyallhostsandroutersonthatnetwork.
* DHCP uses the concept of a *relay agent.* There is at least one relay agent on each network.
* DHCPrelayagentisconfiguredwiththe IPaddressoftheDHCPserver.
* When a relay agent receives a DHCPDISCOVER message, it unicasts it to the DHCP server and awaits the response, which it will then send back tothe requesting client.



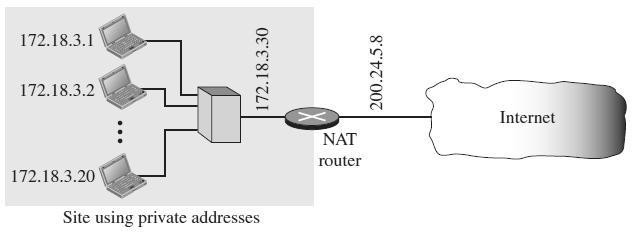
#### DHCPMessageFormat

* + ADHCPpacketisactuallysentusingaprotocolcalledthe*UserDatagram Protocol* (UDP).



**6. NETWORKADDRESSTRANSLATION (NAT)**

* + A technology that can provide the mapping between the private and universal (external)addresses,andatthesametimesupportvirtualprivatenetworksis called as **Network Address Translation (NAT).**
  + The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) forcommunication with the rest of the world.
  + The site must have only one connection to the global Internet through a NAT- capable router that runs NAT software.



* + Theprivatenetworkusesprivateaddresses.
  + Therouterthatconnectsthenetworktotheglobaladdressusesoneprivate address and one global address.
  + TheprivatenetworkisinvisibletotherestoftheInternet;therestoftheInternet sees only the NAT router with the address 200.24.5.8.

#### TypesofNAT

* + TwotypesofNATexists.
    1. One-to-onetranslationofIPaddresses
    2. One-to-manytranslationofIPaddresses

#### AddressTranslation

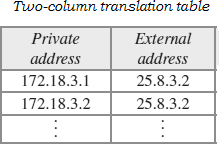
* + AlloftheoutgoingpacketsgothroughtheNATrouter,whichreplacesthe source address in the packet with the global NAT address.
  + All incoming packets also pass through the NAT router, which replaces the destinationaddressinthepacket(theNATrouterglobaladdress)withthe appropriate private address.

#### TranslationTable

* + There may be tens or hundreds of private IP addresses, each belonging to one specific host.
  + Theproblemariseswhenwewantto translatethesourceaddresstoanexternal address. This is solved if the NAT router has a translation table.

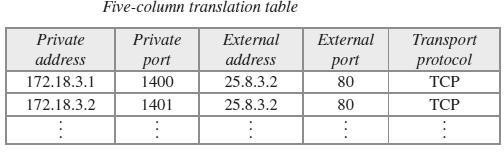
Translationtablewithtwocolumns

* A translation table has only two columns: the private address and the external address (destination address of the packet).
* Whentheroutertranslatesthesourceaddressoftheoutgoingpacket,italso makes note of the destination address—where the packet is going.
* When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet.



Translationtablewithfivecolumns

* To allow a many-to-many relationship between private-network hosts and externalserverprograms,weneedmoreinformationinthetranslationtable.
* If the translation table has five columns, instead of two, that include the source anddestinationportaddressesandthetransport-layerprotocol,theambiguityis eliminated.



**7. FORWARDING OF IPPACKETS**

* + Forwarding means to deliver the packet to the next hop (which can be the final destination or the intermediate connecting device).
  + Although IP protocol was originally designed asaconnectionlessprotocol,today the tendency is to use IP as a connection-oriented protocol based on the label attached to an IP datagram .
  + When***IPisusedasaconnectionlessprotocol***,forwardingisbasedonthe

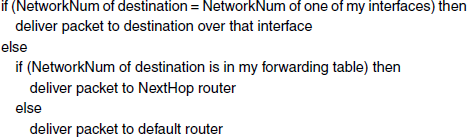
***destinationaddress***oftheIPdatagram.

* + Whenthe***IPisusedasaconnection-oriented protocol***, forwardingisbasedon the ***label*** attached to an IP datagram.

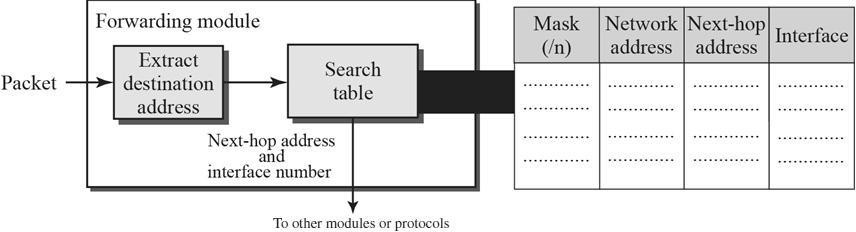
FORWARDINGBASEDONDESTINATIONADDRESS

* Thisisatraditionalapproach.
* Inthiscase,forwardingrequiresahostoraroutertohaveaforwardingtable.
* When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.
* ThemainpointsinforwardingofIPPackets(datagram)arethefollowing:
  + EveryIPPacketscontainstheIPaddressofthedestinationhost.
  + The network part of an IP address uniquely identifies a single physicalnetwork that is part of the larger Internet.
  + Allhostsandroutersthatsharethesamenetworkpartoftheiraddress are connected to the same physical network and can thus communicate with each other by sending frames over that network.
  + Every physical network that is part of the Internet has at least one router that, by definition, is also connected to at least one other physical network;this routercan exchangepackets with hosts or routersoneither network.
* ForwardingIPPacketscanthereforebehandledinthefollowingway.
  + APacketsissentfromasourcehosttoadestinationhost,possibly passing through several routers along the way.
  + Any node, whether it is a host or a router, first tries to establish whether it is connected to the same physical network as the destination.
* Todothis,itcomparesthenetworkpartofthedestinationaddresswiththe network part of the address of each of its network interfaces. (Hosts normallyhave only one interface, while routers normally have two or more, since theyare typically connected to two or more networks.)
* If a match occurs, then that means that the destination lies on the same physical networkastheinterface,andthepacketcanbedirectlydeliveredoverthat network that has a reasonable chance of getting the packet closer to its destination.
* Ifthereisnomatch,thenthenodeisnotconnectedtothesamephysical network as the destination node, then it needs to send the packetto a router.
* Ingeneral, each node will havea choice of several routers, and so it needs topickthebestone,oratleastonethathasareasonablechanceofgettingthe datagram closer to its destination.
* Therouterthatitchoosesisknownasthe*nexthop*router.
* Therouterfindsthecorrectnexthopbyconsulting itsforwarding table.The forwarding table is conceptually just a list of (NetworkNum, NextHop) pairs.
* Thereisalsoadefaultrouterthatisusedifnoneoftheentriesinthetable matches the destination’s network number.
* AllPacketsdestinedforhostsnotonthephysicalnetworktowhichthesending host is attached will be sent out through the default router.

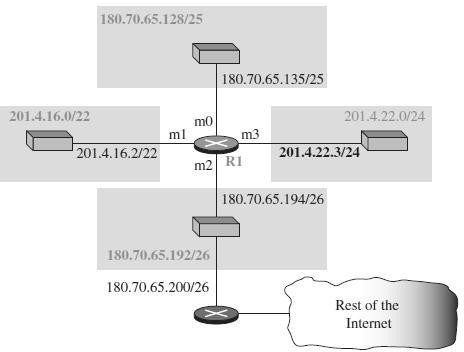
#### ForwardingAlgorithm

****

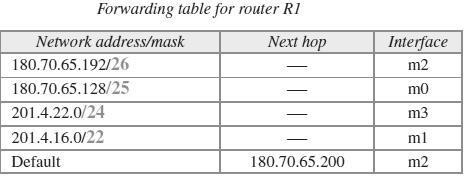
**SimplifiedForwardingModule**

****

* + Thejoboftheforwardingmoduleistosearchthetable, rowbyrow.
  + In each row, the*n*leftmost bits of the destination address (prefix) are kept and the rest of the bits (suffix) are set to 0s.
  + If the resulting address ( *network address*), matches with the address in the first column,theinformationinthenexttwocolumnsisextracted;otherwisethe search continues. Normally, thelast rowhasadefault value in the firstcolumn, which indicates all destination addresses that did not match the previous rows.
  + Routing in classless addressing uses another principle, **longest mask matching.**
  + This principle states that the forwarding table is sorted from the longest maskto the shortest mask.
  + In other words, ifthere arethree masks, /27, /26, and/24, the mask/27 must be the first entry and /24 must be the last.



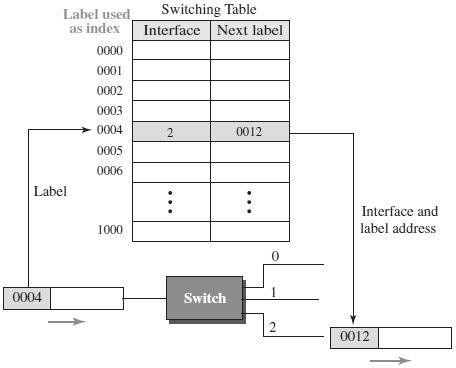
* + Let us make a forwardingtable for router R1 usingthe configuration as given in the figure above



* + When a packet arrives whose leftmost 26 bits in the destination address match the bits in the first row, the packet is sent out from interface m2.
  + When a packet arrives whose leftmost 25 bits in the address match the bits inthe second row, the packet is sent out from interface m0, and so on.
  + The table clearly shows that the first row has the longest prefix and the fourth row has the shortest prefix.
  + The longer prefix means a smaller range of addresses; the shorter prefix means a larger range of addresses.

FORWARDINGBASEDONLABEL

* + Inaconnection-orientednetwork(virtual-circuitapproach),aswitchforwardsa packet based on the label attached to the packet.
  + Routing is normally based on searching the contents of a table; switching can be done by accessing a table using an index.
  + Inotherwords,routinginvolvessearching;switchinginvolvesaccessing.
  + The Figure below shows a simple example of using a label to access a switching table.
  + Sincethelabelsareusedastheindextothetable, findingtheinformationinthe table is immediate.



#### Multi-ProtocolLabelSwitching(MPLS)

* + Duringthe1980s,severalvendorscreatedroutersthatimplementswitching technology.
  + LaterIETFapprovedastandardthatiscalledMulti-ProtocolLabelSwitching.
  + In this standard, some conventional routers in the Internet can be replaced byMPLS routers, which can behave like a router and a switch.
  + When behaving like a router, MPLS can forward the packet based on the destinationaddress; when behavinglike a switch,it canforward apacket based on the label.



**8.NETWORKLAYERPROTOCOLS:IP,ICMPV4**

* The main protocol Internet Protocol is responsible for packetizing, forwarding, and delivery of a packet at the network layer.
* The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.

**IP-INTERNETPROTOCOL**

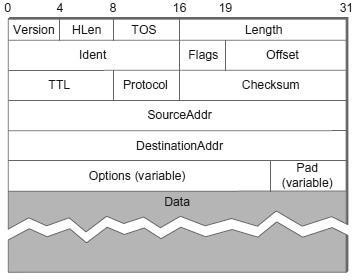
* + The Internet Protocol is the key tool used today to build scalable, heterogeneous internetworks.
  + IPrunsonallthenodes(bothhostsandrouters)inacollectionofnetworks
  + IPdefinestheinfrastructurethatallowsthesenodesandnetworkstofunction as a single logical internetwork.

IPSERVICEMODEL

* + ServiceModeldefinesthehost-to-hostservicesthatwewanttoprovide
  + The main concern in defining a service model for an internetwork is that we can provideahost-to-hostserviceonlyifthisservicecansomehowbeprovidedover each of the underlying physical networks.
* The Internet Protocol is the key tool used today to build scalable, heterogeneous internetworks.
  + The**IPservicemodel**canbethoughtofashaving**twoparts**:
    - A ***GLOBAL ADDRESSING SCHEME*** - which provides a way to identify all hosts in the internetwork
    - A***DATAGRAM DELIVERY MODEL*** – A connectionless model of data delivery.

IPPACKETFORMAT/IPDATAGRAM FORMAT

* + AkeypartoftheIPservicemodelisthetypeofpacketsthatcanbecarried.
  + TheIPdatagramconsistsof aheaderfollowedbyanumberofbytesofdata.



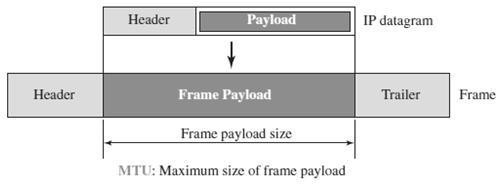
|  |  |
| --- | --- |
| **FIELD** | **DESCRIPTION** |
| ***Version*** | SpecifiestheversionofIP.Twoversionsexists–IPv4andIPv6. |
| ***HLen*** | Specifiesthelengthoftheheader |
| ***TOS***  ***(***Typeof Service) | An indication oftheparametersofthequalityofservice desiredsuchasPrecedence,Delay,ThroughputandReliability. |
| ***Length*** | Lengthoftheentiredatagram,includingtheheader.Themaximum size of an IP datagram is65,535(210)bytes |
| **Ident (Identification)** | Uniquelyidentifiesthepacketsequencenumber. Usedfor fragmentation and re-assembly. |

|  |  |
| --- | --- |
| **Flags** | Usedtocontrolwhetherroutersareallowedtofragmentapacket.  If a packet is fragmented , this flag value is 1.If not, flag value is 0. |
| **Offset (Fragmentation offset)** | Indicateswhereinthedatagram,thisfragmentbelongs.  Thefragmentoffsetismeasuredinunitsof8octets (64bits). The first fragment has offset zero. |
| **TTL**  **(TimetoLive)** | Indicatesthemaximumtimethedatagramisallowedto  remaininthenetwork.Ifthisfield containsthevaluezero, then the datagram must be destroyed. |
| **Protocol** | Indicatesthenextlevelprotocolusedinthedataportionofthe datagram |
| **Checksum** | Usedtodetecttheprocessingerrorsintroduced intothepacket |
| **SourceAddress** | TheIPaddressoftheoriginalsenderofthepacket. |
| **Destination Address** | TheIPaddressofthefinaldestinationofthepacket. |
| **Options** | This is optional field. These options may contain values for options such as Security, Record Route, Time Stamp, etc |
| **Pad** | Usedtoensurethattheinternetheaderendsona32bitboundary. Thepadding is zero. |

**IPDATAGRAM-FRAGMENTATIONANDREASSEMBLY**

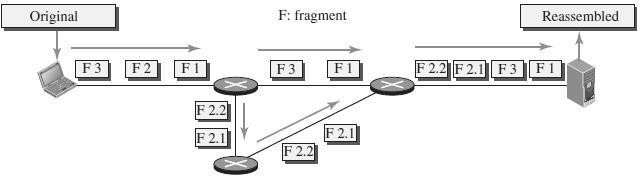
#### Fragmentation:

* + Everynetwork typehasa***maximumtransmissionunit***(MTU),whichis the largest IP datagram that it can carry in a frame.

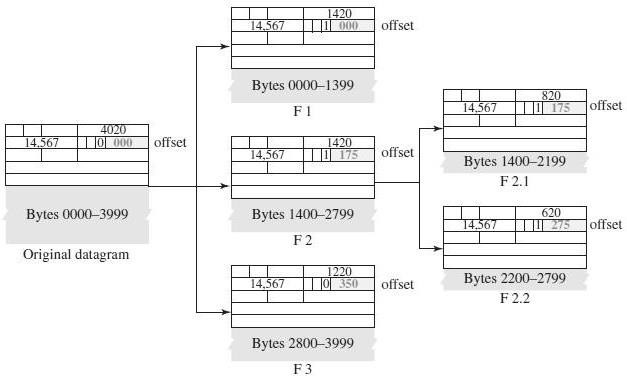


* + Fragmentationofadatagram willonlybenecessaryifthepathtothe destination includes a network with a smaller MTU.
  + WhenahostsendsanIPdatagram,itcanchooseanysizethatitwants.
  + Fragmentation typically occurs in a router when it receives a datagram that itwantstoforwardoveranetworkthathasanMTUthatissmallerthanthe received datagram.
  + Each fragment is itself a self-contained IP datagram that is transmitted over asequence of physical networks, independent of the other fragments.
  + EachIPdatagramisre-encapsulatedforeachphysicalnetworkoverwhichit travels.
  + For example , if weconsider an Ethernetnetwork to accept packets up to 1500 bytes long.
  + ThisleavestwochoicesfortheIPservicemodel:
    - MakesurethatallIPdatagramsaresmallenoughtofitinsideonepacket on any network technology
    - Provide a means by which packets can be fragmented and reassembled when they are too big to go over a given network technology.
  + Fragmentation produces smaller, valid IP datagrams that can be readily reassembled into the original datagram upon receipt, independent of the order of their arrival.

#### Example:

****

* + Theoriginalpacketstartsattheclient;thefragmentsarereassembledatthe server.
  + The value of the identification field is the same in all fragments, as is the value of the flags field with the more bit set for all fragments except the last.
  + Also,thevalueoftheoffsetfieldforeachfragmentisshown.
  + Althoughthefragmentsarrivedoutoforderatthedestination,theycanbe correctly reassembled.



* + Thevalueoftheoffsetfieldisalwaysrelativetotheoriginaldatagram.
  + Evenifeachfragmentfollowsadifferentpathandarrivesoutoforder,the finaldestinationhostcanreassembletheoriginaldatagramfromthe fragments received (if none of them is lost) using the following strategy:

1. Thefirstfragmenthasanoffsetfieldvalueofzero.
2. Divide the length of the first fragment by 8. The second fragment has an offset value equal to that result.
3. Divide the total length of the first and second fragment by 8. The thirdfragment has an offset value equal to that result.
4. Continuetheprocess.ThelastfragmenthasitsMbitsetto0.
5. Continuetheprocess.Thelastfragmenthasa*more*bitvalueof0.

#### Reassembly:

* + Reassemblyisdoneatthereceivinghostandnotateachrouter.
  + Toenablethesefragmentstobereassembledatthereceivinghost,theyall carry the same identifier in the Ident field.
  + This identifier is chosen by the sending host and is intendedtobeunique among all the datagramsthat might arriveat the destination from this sourceover some reasonable time period.
  + Sinceallfragmentsof theoriginaldatagramcontain this identifier,the reassemblinghostwillbeabletorecognizethosefragmentsthatgotogether.
  + For example, if a single fragment is lost, the receiver will still attempt to reassemble the datagram, and it will eventually give up and have togarbage-collect the resources that were used to perform the failed reassembly.
  + Hosts are now strongly encouraged to perform “path MTU discovery,”aprocess by which fragmentation is avoided by sending packets that are smallenough to traverse the link with the smallest MTU in the path from sender toreceiver.

IPSECURITY

TherearethreesecurityissuesthatareparticularlyapplicabletotheIPprotocol:

(1)PacketSniffing(2)PacketModification and(3)IP Spoofing.

#### PacketSniffing

* + AnintrudermayinterceptanIPpacketandmakeacopyof it.
  + Packetsniffing isapassiveattack,inwhichtheattackerdoesnotchangethe contents of the packet.
  + Thistypeofattackisverydifficulttodetectbecausethesenderandthereceiver may never know that the packet has been copied.
  + Although packet sniffingcannot be stopped,encryption of thepacket can make the attacker’s effort useless.
  + Theattackermaystillsniffthepacket,butthecontentisnotdetectable.

#### PacketModification

* + Thesecondtypeofattackistomodifythepacket.
  + Theattackerinterceptsthepacket,changesitscontents,andsendsthenew packet to the receiver.
  + Thereceiverbelievesthatthepacketiscomingfromtheoriginalsender.
  + Thistypeofattackcanbedetectedusingadataintegritymechanism.
  + Thereceiver,beforeopeningandusingthecontentsofthemessage,canuse this mechanism to make sure that the packet has not been changed during thetransmission.

#### IPSpoofing

* + AnattackercanmasqueradeassomebodyelseandcreateanIPpacketthat carries the source address of another computer.
  + An attacker can send an IP packet to a bank pretending that it is coming fromone of the customers.
  + Thistypeofattackcanbepreventedusinganoriginauthentication mechanism

#### IPSec

* + The IP packets today can be protected from the previously mentioned attacksusing a protocol called IPSec (IP Security).
  + ThisprotocolisusedinconjunctionwiththeIPprotocol.
  + IPSecprotocolcreatesaconnection-orientedservicebetweentwoentitiesin which they can exchange IP packets without worrying about the three attackssuch asPacket Sniffing, Packet Modificationand IP Spoofing.
  + IPSecprovidesthefollowingfourservices:

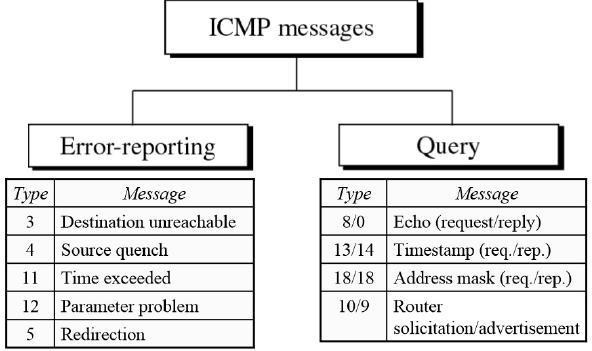
1. **Defining Algorithms and Keys :** The two entities that want to create a secure channel between themselves can agree on some available algorithms and keys to be used for security purposes.
2. **Packet Encryption :**The packets exchanged between two parties canbe encrypted for privacy using one of the encryption algorithms and a shared key agreed upon in the first step. This makes the packet sniffing attack useless.
3. **Data Integrity :** Data integrity guarantees that the packet isnot modified during the transmission. If the received packet does not passthedataintegritytest,itisdiscarded.Thispreventsthesecondattack, packet modification.
4. **Origin Authentication :** IPSec can authenticate the originofthepackettobesurethatthepacketisnotcreated byanimposter. Thiscan prevent IP spoofing attacks.

**ICMPV4-INTERNETCONTROLMESSAGEPROTOCOLVERSION4**

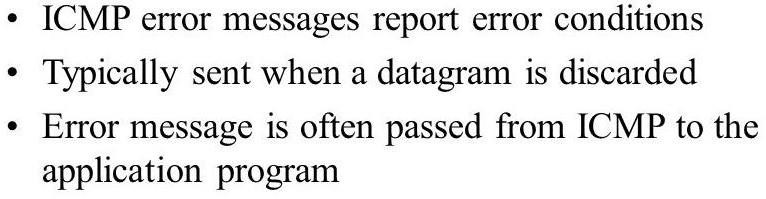
* + ICMPisanetwork-layerprotocol.
  + ItisacompaniontotheIPprotocol.
  + InternetControlMessageProtocol(ICMP)definesacollectionoferror messagesthataresentbacktothesourcehostwheneverarouterorhostis unable to process an IP datagram successfully.

ICMPMESSAGETYPES

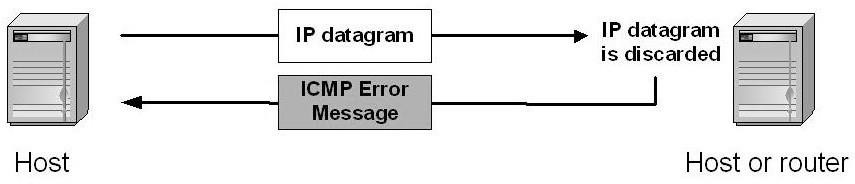
* + ICMPmessagesaredividedintotwobroadcategories:*error-reporting messages* and *query messages.*
  + Theerror-reportingmessagesreportproblemsthatarouterorahost (destination) may encounter when it processes an IP packet.
  + The query messages help a host or a network manager get specific information from a router or another host.



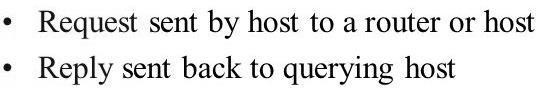
#### ICMPError–ReportingMessages

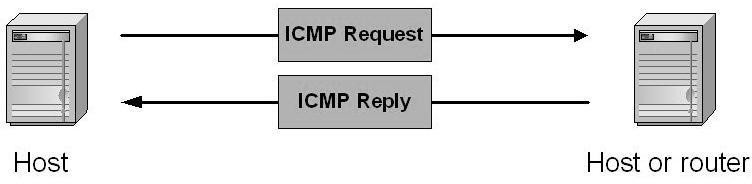


* ***Destination Unreachable****―*When a router*cannot route*a datagram, the datagram is discarded and sends a destination unreachable message to source host.
* ***Source Quench****―*When a router or host discards a datagram due to *congestion*, it sends a source-quench message to the source host. This message acts as flow control.
* ***Time Exceeded****―*Router discards a datagram when TTL field becomes 0 and a time exceeded message is sent to the source host.
* ***ParameterProblem****―*Ifarouterdiscoversambiguousor*missing*valueinany field of the datagram, it discards the datagram and sends parameter problem message to source.
* ***Redirection****―*Redirect messagesaresentbythedefaultroutertoinformthesource host to *update* its forwarding table when the packet is routed on a wrong path.



#### ICMPQueryMessages

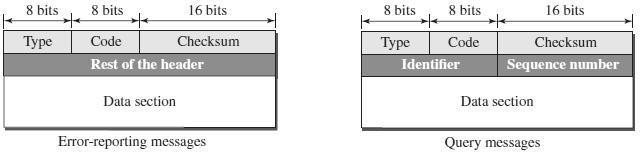




* + ***EchoRequest&Reply***―Combinationofechorequestandreplymessages determines whether two systems communicate or not.
  + ***TimestampRequest&Reply***―Twomachinescanuse thetimestamprequest and reply messages to determine the round-trip time (RTT).
  + ***Address Mask Request & Reply***―A host to obtain its subnet mask, sends anaddressmask requestmessagetotherouter,whichrespondswithanaddress mask reply message.
  + ***Router Solicitation/Advertisement***―A host broadcasts a router solicitation messagetoknowabouttherouter.Routerbroadcastsitsroutinginformation with router advertisement message.

ICMPMESSAGEFORMAT

* + AnICMPmessagehasan8-byteheaderandavariable-sizedatasection.



|  |  |
| --- | --- |
| Type | Definesthetypeofthemessage |
| Code | Specifiesthereasonfortheparticularmessagetype |
| Checksum | Usedforerrordetection |
| Restofthe header | Specificforeachmessagetype |
| Data | Usedtocarryinformation |
| Identifier | Usedtomatchtherequestwiththereply |
| SequenceNumber | SequenceNumberoftheICMPpacket |

ICMPDEBUGGINGTOOLS

Twotoolsareusedfordebuggingpurpose.Theyare(1)Ping(2) Traceroute

#### Ping

* + The*ping*programisusedtofindifahostisaliveand responding.
  + The source host sends ICMP echo-request messages; the destination, if alive,responds with ICMP echo-reply messages.
  + The *ping* program setstheidentifierfieldin theecho-requestandecho-reply message and starts the sequence number from0; this number is incremented by 1 each time a new message is sent.
  + The*pingprogram*cancalculatetheround-triptime.
  + Itinsertsthesendingtimeinthedatasectionofthemessage.
  + When the packet arrives, it subtracts the arrival time fromthe departure time to get the round-trip time (RTT).

**$pinggoogle.com**

#### TracerouteorTracert

* + The*traceroute*program in UNIX or*tracert*in Windows can be used to trace the path of a packet from a source to the destination.
  + ItcanfindtheIPaddressesofalltheroutersthatarevisitedalongthepath.
  + Theprogramis usuallysettocheckforthe maximumof30hops(routers)tobe visited.
  + ThenumberofhopsintheInternetisnormallylessthanthis.

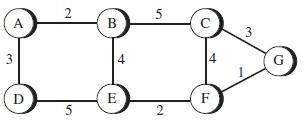
$traceroutegoogle.com

**9. UNICASTROUTING**

* Routingistheprocessofselectingbestpathsinanetwork.
* Inunicastrouting, apacket isrouted, hopbyhop, fromitssourcetoits destination by the help of forwarding tables.
* Routingapacketfromitssourcetoitsdestinationmeansroutingthepacket froma*sourcerouter*(thedefaultrouterofthesourcehost)toa*destination router* (the router connected to the destination network).
* The source host needs no forwarding table because it delivers its packet to the default router in its local network.
* Thedestinationhostneedsno forwarding tableeitherbecauseit receivesthe packet from its default router in its local network.
* Onlytheintermediateroutersinthenetworksneedforwardingtables.

NETWORKASAGRAPH

* + TheFigurebelowshowsagraphrepresentinganetwork.



* + The nodes of the graph, labeled A through G, may be hosts, switches, routers, or networks.
  + Theedgesofthegraphcorrespondtothenetworklinks.
  + Eachedgehasanassociated*cost.*
  + The basic problem of routing is to find the lowest-cost path between any twonodes, where the cost of a path equals the sumof the costs of all the edges that make up the path.
  + Thisstaticapproachhasseveralproblems:
    - Itdoesnotdealwithnodeorlinkfailures.
    - Itdoesnotconsidertheadditionofnewnodesorlinks.
    - Itimpliesthatedgecostscannotchange.
  + For these reasons, routing is achieved by running routing protocols among the nodes.
  + Theseprotocolsprovideadistributed,dynamicwaytosolvetheproblemof findingthelowest-costpathinthepresenceoflinkandnodefailuresandchanging edge costs.

## UNICASTROUTINGALGORITHMS

* Therearethreemainclassesofroutingprotocols:

1. **DistanceVectorRoutingAlgorithm–RoutingInformationProtocol**
2. **LinkStateRoutingAlgorithm–OpenShortestPathFirstProtocol**
3. **Path-VectorRoutingAlgorithm-BorderGatewayProtocol**

**DISTANCE VECTOR ROUTING (DSR) ROUTINGINFORMATIONPROTOCOL(RIP) BELLMAN - FORD ALGORITHM**

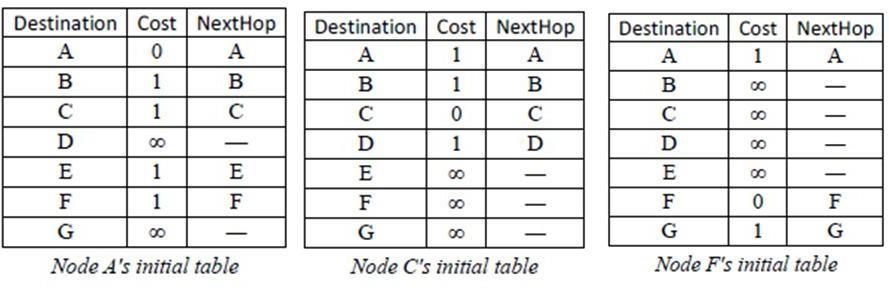
* + Distancevectorroutingis*distributed*,i.e.,algorithmisrunonallnodes.
  + Eachnode*knows*thedistance(cost)toeachofitsdirectlyconnectedneighbors.
  + Nodesconstructa*vector*(Destination,Cost,NextHop)anddistributestoits neighbors.
  + Nodescomputeroutingtableof*minimum*distancetoeveryothernodevia NextHop using information obtained from its neighbors.

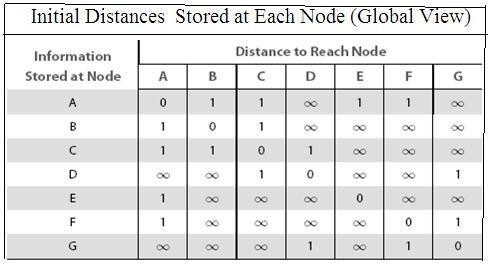
#### InitialState

* + Ingivennetwork, *cost*ofeachlinkis1 hop.
  + Eachnodesetsadistanceof1(hop)toits*immediate*neighborand cost to itselfas 0.
  + Distancefornon-neighborsismarkedas*unreachable*withvalue∞(infinity).
  + Fornode*A*,nodes*B*,*C*,*E*and*F*are*reachable*,whereasnodes*D*and*G*

are*unreachable*.

* + Theinitialtableforallthenodesaregivenbelow

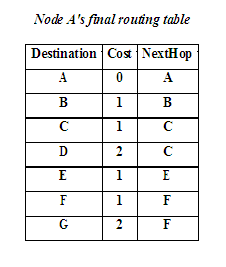




* + Eachnode*sends*itsinitialtable(distancevector)toneighborsandreceives their estimate.
  + Node*A* sends its table to nodes*B*, *C*, *E* &*F* and receives tables from nodes*B*, *C*, *E* &*F*.
  + Each node*updates* its routing table by comparing with each of its neighbor'stable
  + Foreachdestination,TotalCostiscomputed as:
* ***TotalCost***=Cost(*Node*to*Neighbor*)+Cost(*Neighbor*to*Destination*)
  + IfTotalCost<Cost then
* ***Cost***=TotalCostandNextHop=*Neighbor*
  + Node*A learns* from*C*'s table to reach node*D* and from*F*'s table to reach node *G*.
  + TotalCosttoreachnode *D*via*C*=Cost(*A*to*C*)+Cost(*C*to*D*)

Cost=1+1=2.

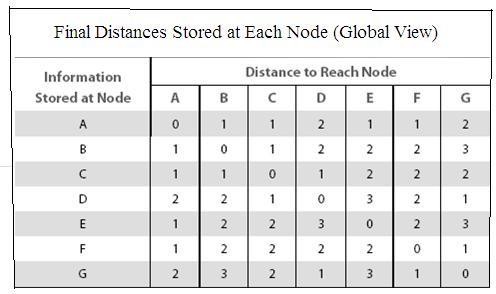
* Since2<∞,entryfordestination*D*in*A*'stableischangedto(*D*,2, *C*)
* TotalCosttoreachnode*G*via*F*=Cost(*A*to*F*)+Cost(*F*to*G*)=1+1=2
* Since2<∞,entryfordestination*G*in*A*'stableischangedto(*G*,2, *F*)
  + Each node builds*complete* routingtable after few exchanges amongst its neighbors.



* + Systemstabilizeswhenallnodeshavecompleteroutinginformation,i.e.,

convergence.

* + Routingtablesareexchanged*periodicallyor*incaseof*triggered update*.
  + Thefinaldistancesstoredateachnodeisgiven below:



#### UpdationofRoutingTables

Therearetwodifferentcircumstancesunderwhichagivennodedecidestosenda routing update to its neighbors.

***PeriodicUpdate***

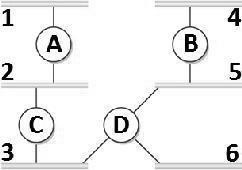
* Inthiscase,eachnodeautomatically sendsan updatemessageevery sooften, even if nothing has changed.
* The frequency of these periodic updates varies from protocol to protocol, but it is typically on the order of several seconds to several minutes.

***TriggeredUpdate***

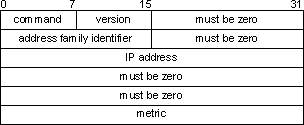
* + In this case, whenever a node notices a link failure or receives an update from oneofitsneighborsthatcausesittochangeoneoftheroutesinitsrouting table.
  + Whenever a node’s routing table changes, it sends an update to its neighbors,which may lead to a change in their tables, causing them to send an update totheir neighbors.

### ROUTINGINFORMATIONPROTOCOL(RIP)

* RIPisanintra-domainroutingprotocolbasedondistance-vectoralgorithm.

Example

* Routers *advertise* the cost of reaching networks. Cost of reaching each link is 1 hop. For example, router*C*advertises to*A* thatit canreach network2, *3*atcost 0 (directly connected), networks *5*, *6* at cost 1 and network *4* at cost 2.
* Eachrouter*updates*costandnexthopforeachnetworknumber.
* Infinity is defined as 16, i.e., any route cannothave more than 15 hops. Therefore RIP can be implemented on small-sized networks only.
* Advertisementsaresentevery30secondsorincaseoftriggeredupdate.



* + ***Command***-Itindicatesthepackettype.

Value1representsarequestpacket.Value2representsaresponsepacket.

* + ***Version***-ItindicatestheRIPversionnumber.ForRIPv1,thevalueis0x01.
  + ***AddressFamilyIdentifier***-Whenthevalueis2,itrepresentstheIPprotocol.
  + ***IPAddress***-ItindicatesthedestinationIPaddress oftheroute. Itcanbethe addresses of only the natural network segment.
  + ***Metric***-Itindicatesthehopcountofaroutetoits destination.

#### Count-To-Infinity(or)LoopInstabilityProblem

* Supposelinkfromnode*A*to*E*goes*down*.
  + Node*A*advertisesadistanceof∞to*E*toitsneighbors
  + NodeBreceivesperiodicupdatefromCbeforeA’supdate reaches B
  + Node*B*updatedby*C*,concludesthat*E*canbereachedin3hopsvia*C*
  + Node*B*advertisesto*A*as3hopstoreach*E*
  + Node*A*inturnupdates*C*withadistanceof4hopsto*E*andsoon
* Thusnodesupdateeachotheruntilcostto*E*reaches*infinity*,i.e.,*no convergence*.
* Routingtabledoesnotstabilize.
* Thisproblemiscalled*loopinstability*or*counttoinfinity*

SolutiontoCount-To-Infinity(or)LoopInstabilityProblem:

* *Infinity*isredefinedtoasmallnumber,say16.
* Distancebetweenanytwonodescanbe15hopsmaximum.Thusdistance vector routing *cannot be used* in large networks.
* Whenanodeupdatesitsneighbors,itdoesnotsendthoseroutesitlearned from each neighbor back to that neighbor. This is known as **split horizon**.
* **Splithorizonwithpoison reverse**allowsnodestoadvertiseroutesitlearnt from a node back to that node, but with a warning message.

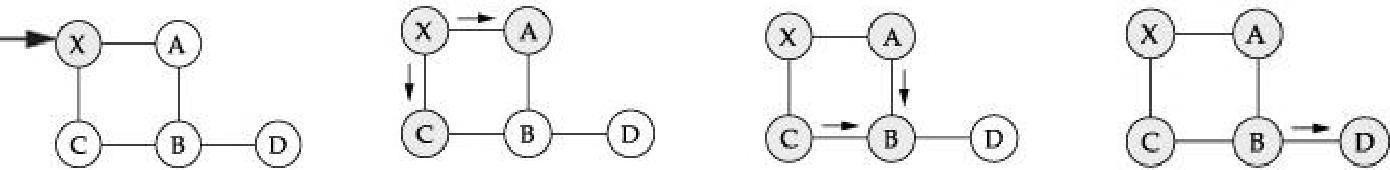
**LINKSTATEROUTING (LSR)**

**OPENSHORTESTPATHPROTOCOL(OSPF) DIJKSTRA’SALGORITHM**

* Eachnodeknows*state*oflinktoitsneighborsand*cost*.
* Nodescreateanupdatepacketcalled*link-statepacket*(LSP)thatcontains:
* IDofthenode
* Listofneighborsforthatnodeandassociatedcost
* 64-bitSequencenumber
* Timetolive
* Link-Stateroutingprotocolsrelyontwomechanisms:
* ***Reliableflooding***oflink-stateinformationtoallothernodes
* ***Routecalculation***fromtheaccumulatedlink-stateknowledge

#### ReliableFlooding

* Eachnode*sends*itsLSPoutoneachofitsdirectlyconnected links.
* When a node receives LSP of another node, checks if it has an LSP already for that node.
* Ifnot,itstoresandforwardstheLSPonallotherlinksexcepttheincoming one.
* ElseifthereceivedLSPhasa*bigger*sequencenumber,thenitis storedand forwarded. Older LSP for that node is *discarded*.
* OtherwisediscardthereceivedLSP,sinceitisnotlatestforthatnode.
* ThusrecentLSPofanodeeventually*reaches*allnodes,i.e.,reliable*flooding*.



(a) (b) (c) (d)

* FloodingofLSPinasmallnetworkisasfollows:
* Whennode*X*receives*Y*’s LSP(*figa*),itfloodsontoitsneighbors*A*

and*C*(*figb*)

* Nodes*A*and*C*forwarditto*B*,butdoesnotsendsitbackto*X*(*figc*).
* Node*B*receivestwocopiesofLSPwithsamesequencenumber.
* AcceptsoneLSPandforwardsitto*D*(*figd*).Floodingiscomplete.
* LSPisgeneratedeither*periodically*orwhenthereisa*change*inthetopology.

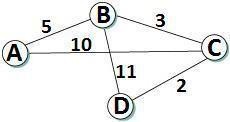
#### RouteCalculation

* Eachnodeknowstheentiretopology,onceithasLSPfromeveryothernode.
* Forward search algorithm is used to compute routing table from the receivedLSPs.
* Each node maintains two lists, namely Tentative and Confirmed with entries of the form (Destination, Cost, NextHop).

DIJKSTRA’SSHORTESTPATHALGORITHM (FORWARD SEARCH ALGORITHM)

1. Eachhostmaintainstwolists,knownas***Tentative***and***Confirmed***
2. InitializetheConfirmedlistwithanentryfortheNode(Cost=0).
3. NodejustaddedtoConfirmedlistiscalledNext.ItsLSPisexamined.
4. For each neighbor of Next,calculate costto reach each neighbor as Cost (Node to Next) + Cost (Next to Neighbor).
   1. If Neighbor isneither inConfirmed nor in Tentative list, then add (Neighbor, Cost, NextHop) to Tentative list.
   2. If Neighbor is in Tentative list, and Cost is less than existing cost, then replace the entry with (Neighbor, Cost, NextHop).
5. IfTentativelistisemptythen*Stop*,otherwisemove *least*costentryfrom Tentative list to Confirmed list. Go to *Step 2*.

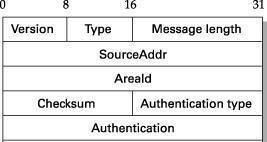
**Example :**



### OPENSHORTESTPATHFIRSTPROTOCOL(OSPF)

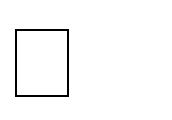
* OSPFisanon-proprietarywidelyusedlink-stateroutingprotocol.
* OSPFFeaturesare:
  + **Authentication**―Malicious host can collapse a network by advertising to reach every host with cost 0. Such disasters are averted by authenticating routing updates.
  + **Additional hierarchy**―Domain is partitioned into areas, i.e., OSPF is more scalable.
  + **Load balancing**―Multiple routes to the same place are assigned same cost. Thus traffic is distributed evenly.

#### LinkStatePacketFormat

****

***Version***―representsthecurrentversion,i.e.,2.

***Type***―representsthetype(1–5)ofOSPFmessage.



T*ype 1* - “hello” message, T*ype 2* - request, T*ype3*–send, T*ype 4* - acknowledge the receipt of link state messages ,

T*ype5* -reserved

***SourceAddr***―identifiesthesender



***AreaId***―32-bitidentifieroftheareainwhichthenodeislocated

***Checksum***―16-bitinternetchecksum

***Authenticationtype***―1(simplepassword),2(cryptographicauthentication).

***Authentication***―containspasswordorcryptographicchecksum

#### DifferenceBetweenDistance-VectorAndLink-StateAlgorithms

***LinkstateRouting***

Each node talks to all other nodes, but it tells them only what it knows for sure (i.e., only the state of its directly connected links).

***Distance vector Routing*** Eachnodetalksonlytoitsdirectly connectedneighbors,butittellsthem everything it has learned

(i.e.,distancetoallnodes).

**PATH VECTORROUTING (PVR) BORDERGATEWAYPROTOCOL(BGP)**

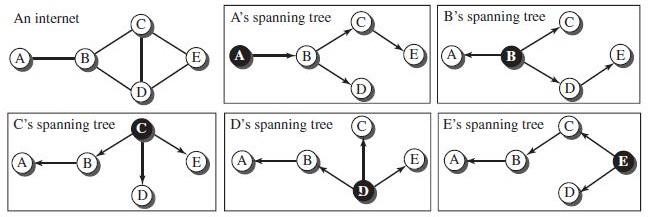
* Path-vectorroutingisanasynchronousanddistributedroutingalgorithm.
* ThePath-vectorroutingisnotbasedonleast-costrouting.
* The best route is determined by the source using the policy it imposes on theroute.
* Inotherwords,thesourcecancontrolthepath.
* Path-vectorroutingisnotactuallyusedinaninternet,andismostlydesignedto route a packet between ISPs.

#### SpanningTrees

* In path-vector routing, the path from a source to all destinations is determined by the *best* spanning tree.
* Thebestspanningtreeisnottheleast-costtree.
* Itisthetreedeterminedbythesourcewhenitimposesitsownpolicy.
* If there is more than one route to a destination, the source can choose the route that meets its policy best.
* Asourcemayapplyseveralpoliciesatthesametime.
* One of the common policies uses the minimum number of nodes to be visited. Anothercommonpolicyistoavoidsomenodesasthemiddlenodeinaroute.
* The spanning trees are made, gradually and asynchronously, byeachnode.When a node is booted, it creates a*path vector*based on the information it can obtain about its immediate neighbor.
* Anodesendsgreetingmessagestoitsimmediateneighborstocollectthese pieces of information.
* Eachnode, afterthecreationoftheinitialpath vector, sendsittoallits immediate neighbors.
* Eachnode,whenitreceivesapathvectorfromaneighbor,updatesitspath vector using the formula
* Thepolicyisdefinedbyselectingthe*best*ofmultiplepaths.
* Path-vectorroutingalsoimposesonemoreconditiononthisequation.
* IfPath(**v**, ***y***)includes***x***,thatpathisdiscardedtoavoidaloopinthe path.
* Inotherwords,***x***doesnotwanttovisititselfwhenitselectsapathto***y***.

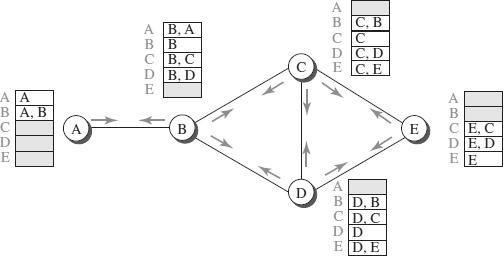
Example:

* TheFigurebelowshowsasmallinternetwithonlyfivenodes.
* Eachsourcehascreateditsownspanningtreethatmeetsitspolicy.
* The policy imposed by all sources is to use the minimum number of nodes toreach a destination.
* Thespanningtree selectedby AandE issuchthat the communicationdoes not pass through D as a middle node.
* Similarly, the spanning tree selected by B is such that the communication does not pass through C as a middle node.



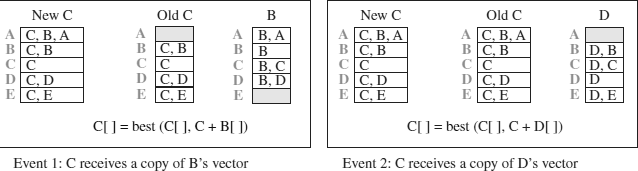
#### PathVectorsmadeatbootingtime

* TheFigurebelowshowsallofthesepathvectorsforthe example.
* Notallofthesetablesarecreatedsimultaneously.
* Theyarecreatedwheneachnodeisbooted.
* The figure also shows how these path vectors are sent to immediate neighbors after they have been created.



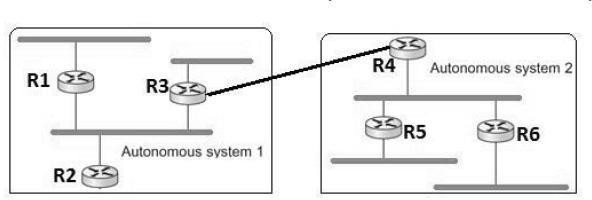
#### UpdatingPathVectors

* TheFigurebelowshowsthepathvectorofnodeCaftertwoevents.
* Inthefirstevent,nodeCreceivesacopyofB’svector,whichimprovesits vector: now it knows how to reach node A.
* Inthesecondevent,nodeCreceivesacopyofD’svector,whichdoesnot change its vector.
* ThevectorfornodeCafterthefirsteventisstabilizedandservesasits forwarding table.

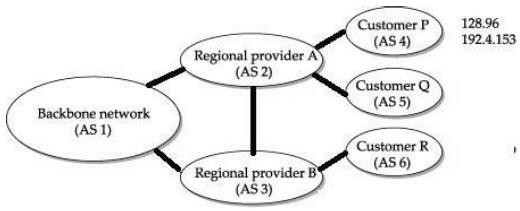


### BORDERGATEWAYPROTOCOL(BGP)

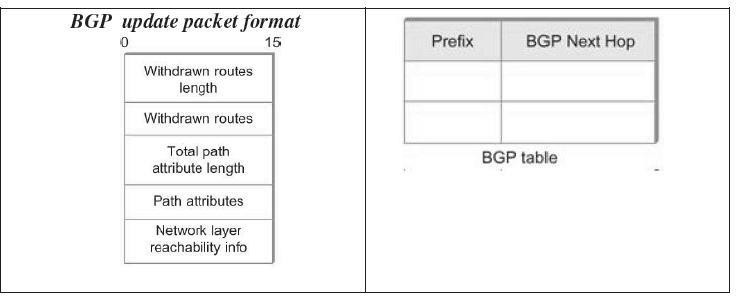
* The Border Gateway Protocolversion (BGP)is the only interdomain routingprotocol used in the Internet today.
* BGP4 is based on the path-vector algorithm. It provides information about the reachability of networks in the Internet.
* BGPviewsinternetasasetofautonomoussystemsinterconnected arbitrarily.



* EachAShavea*borderrouter*(gateway),bywhichpacketsenterandleavethat AS. In above figure, *R3* and *R4* are border routers.
* OneoftherouterineachautonomoussystemisdesignatedasBGP*speaker*.
* BGPSpeaker*exchange*reachabilityinformationwithotherBGPspeakers, known as *external* BGP session.
* BGPadvertisescomplete*path*asenumeratedlistofAS(path vector)toreacha particular network.
* Pathsmustbewithoutany*loop,*i.e.,ASlistisunique.
* For*example*,backbonenetworkadvertisesthatnetworks128.96and192.4.153 can be reached along the path <*AS1*, *AS2, AS4*>.



* Ifthereare*multiple*routestoadestination,BGPspeakerchoosesonebasedon policy.
* Speakers*neednot*advertiseanyroutetoadestination,evenifoneexists.
* Advertisedpathscanbe*cancelled*,ifalink/nodeonthepathgoesdown.This negative advertisement is known as *withdrawn* route.
* Routesarenotrepeatedlysent.Ifthereisnochange, *keepalive*messagesare sent.



#### iBGP-interior BGP

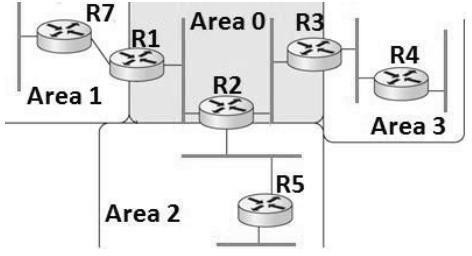
* AVariantofBGP
  + Usedbyrouterstoupdateroutinginformationlearntfromother speakersto routers inside the autonomous system.
  + EachrouterintheASisabletodeterminethe appropriatenexthopforall prefixes.

## 10. UNICASTROUTINGPROTOCOLS

* + Aprotocolismorethananalgorithm.
  + A protocol needs to define its domain of operation, the messages exchanged,communicationbetweenrouters,andinteractionwithprotocolsinother domains.
  + A routing protocol specifies how routers communicate with each other, distributinginformationthatenablesthemtoselectroutesbetweenany two nodes on a computer network.
  + Routers perform the "traffic directing" functions on the Internet; data packetsareforwardedthroughthenetworksof theinternetfromroutertorouter until they reach their destination computer.
  + Routingalgorithmsdeterminethespecificchoiceofroute.
  + Eachrouterhasapriorknowledgeonlyofnetworksattachedtoitdirectly.
  + A routing protocol shares this informationfirstamongimmediateneighbors,andthenthroughoutthenetwork.Thisway,routersgainknowledgeofthe topology of the network.
  + The ability of routing protocols to dynamically adjust to changing conditionssuch as disabled data lines and computers and route data around obstructions is what gives the Internet its survivability and reliability.
  + The specific characteristics of routing protocols include themanner in whichtheyavoidroutingloops,themannerinwhichtheyselectpreferredroutes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors.

INTERNETSTRUCTURE

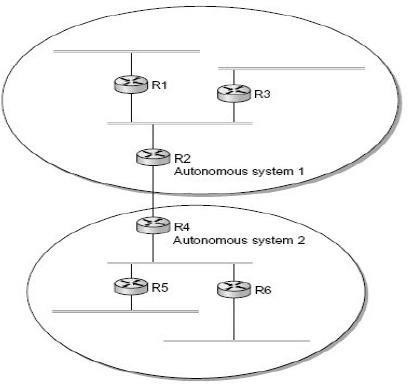
* + Internethasamillionnetworks.Routingtableentriesperroutershouldbe minimized.
  + Linkstateroutingprotocolisusedtopartitiondomaininto*areas*.
  + Anroutingareaisasetofroutersconfiguredtoexchangelink-state information.
  + Areaintroducesanadditionallevelof*hierarchy*.
  + Thusdomainscangrowwithoutburdeningroutingprotocols.



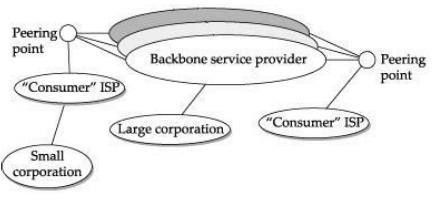
* + Thereisonespecialarea—the***backbonearea***,alsoknownasarea 0.
  + Routers*R1*,*R2*and*R3*arepartofbackbonearea.
  + Routers in backbone area are also part of non-backbone areas. Such routers are known as **A*rea Border Routers*** (ABR).
  + Link-stateadvertisementis*exchanged*amongstroutersinanon-backbonearea.
  + TheydonotseeLSAsofotherareas. Forexample, *area1*routersarenotaware of *area* 3 routers*.*
  + ABR*advertises*routinginformationintheirareatootherABRs.
  + For example,*R2*advertises*area 2*routing information to*R1*and*R3*, which in turn pass onto their areas.
  + Allrouterslearnhowto*reach*allnetworksinthedomain.
  + Whenapacketistobesenttoanetworkinanotherarea,itgoesthrough backbone area via ABR and reaches the destination area.
  + RoutingAreasimprovescalabilitybutpackets may nottravelontheshortest path.

INTERDOMAINROUTING

* + Internet is organized as autonomous systems (AS) each of which is under thecontrol of a single administrative entity.
  + Acorporation’scomplexinternalnetworkmightbeasingleAS,asmaythe network of a single Internet Service Provider (ISP).
  + Interdomainroutingsharesreachabilityinformationbetweenautonomous systems.



* + The basic idea behind autonomous systems is to provide an additional way to hierarchicallyaggregateroutinginformationinalargeinternet,thusimproving scalability.
  + Internethas*backbone*networksand*sites*.Providersconnectatapeeringpoint.



Trafficontheinternetisoftwotypes:

* ***LocalTraffic***-Trafficwithinanautonomoussystemiscalled*local*.
* ***TransitTraffic***-Trafficthatpassesthroughanautonomoussystemiscalled

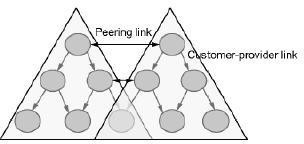
*transit*.

AutonomousSystems(AS)areclassifiedas:

* ***StubAS****-*isconnectedtoonlyoneanotherautonomoussystemandcarries local traffic only (e.g. Small corporation).
* ***Multihomed AS****-*has connections to multiple autonomous systems but refuses to carry transit traffic (e.g. Large corporation).
* ***Transit AS****-*has connections to multiple autonomous systems and is designed to carry transit traffic (e.g. Backbone service provider).

PoliciesUsedByAutonomousSystems:

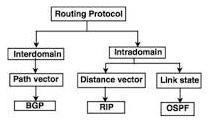
* ***Provider-Customer***―Provider advertises the routes it knows, to the customer and advertises the routes learnt from customer to everyone.
* ***Customer-Provider***―Customers want the routes to be divertedtothem.So theyadvertisetheirownprefixesandrouteslearnedfromcustomerstoprovider and advertise routes learned from provider to customers.
* ***Peer***―Twoprovidersaccesstoeachother’scustomerswithouthavingtopay.



CHALLENGESININTER-DOMAINROUTINGPROTOCOL

* + Each autonomous system has an intra-domain routing protocol, its own policy and metric.
  + Internetbackbone mustbeabletoroutepacketstothedestinationthatcomplies with policies of autonomous system along a loopless path.
  + Service providers have trust deficit and may not trust advertisements by other AS, or may refuse to carry traffic from other AS.

TYPESOFROUTINGPROTOCOLS

****

TwotypesofRoutingProtocolsareusedintheInternet:

1. Intradomainrouting
   * Routingwithinasingleautonomoussystem
   * Routing Information Protocol (RIP) - based on the distance-vector algorithm-(REFERdistance-vectorroutingalgorithm)
   * OpenShortestPathFirst(OSPF)-basedonthelink-statealgorithm-

(REFERlink-stateroutingalgorithm)

1. Interdomainrouting
   * Routingbetweenautonomoussystems.
   * BorderGatewayProtocol(BGP)-basedonthepath-vectoralgorithm-

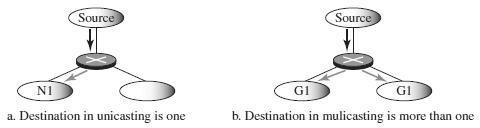
(REFERPathVectorroutingalgorithm)

## 11.MULTICASTING

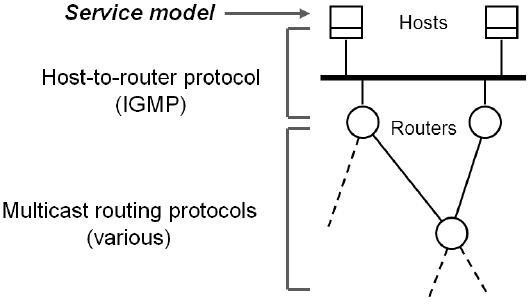
* + In multicasting,thereisonesourceandagroupofdestinations.
  + Multicastsupportsefficientdeliverytomultipledestinations.
  + Therelationshipisonetomanyormany-to-many.
  + **One-to-Many(SourceSpecificMulticast)** oRadio station broadcast oTransmitting news, stock-price oSoftware updates to multiple hosts
  + Many-to-Many(AnySourceMulticast)

oMultimediateleconferencing oOnline multi-player games oDistributed simulations

* + In this type of communication, the source address is a unicast address, but the destination address is a group address.
  + Thegroupaddressdefinesthemembersofthegroup.



* + - In multicasting, a multicast router may have to send out copies of the same datagram through more than one interface.
    - Hoststhatare membersof agroupreceivecopies ofanypacketssent tothat group’s multicast address
    - Ahostcanbeinmultiplegroups
    - Ahostcanjoinandleavegroups
    - A host signals its desire to join or leave a multicast group by communicating with its local router using a special protocol.
    - InIPv4,theprotocolisInternetGroupManagementProtocol(IGMP)
    - InIPv6,theprotocolisMulticastListenerDiscovery(MLD)



IGMPORMLDPROTOCOL

* + - Hosts communicate their desire to*join* /*leave* a multicast group to a router using Internet Group Message Protocol (IGMP) in IPv4 or Multicast Listener Discovery (MLD) in IPv6.
    - Provides multicast routers with information about the membership status of hosts connected to the network.
    - Enablesamulticastroutertocreateandupdatelistofloyalmembersfor each group.

MULTICASTADDRESSING

* + Multicastaddressisassociatedwithagroup,whosemembersaredynamic.
  + EachgrouphasitsownIPmulticastaddress.
  + IP addresses reserved for multicasting are Class D in IPv4 (Class D 224.0.0.1to 239.255.255.255), 1111 1111 prefix in IPv6.

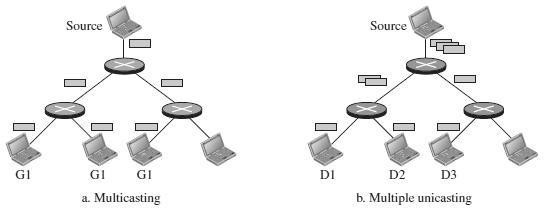
o

* + Hoststhataremembersofagroupreceivecopyofthepacketsentwhen

destinationcontainsgroupaddress.

MULTICASTINGVERSUSMULTIPLEUNICASTING

* + **Multicasting** starts with a single packet from the source that is duplicated bytherouters.Thedestinationaddressineachpacketisthesameforall duplicates.
  + Onlyasinglecopyofthepackettravelsbetweenanytwo routers.



* + In**multipleunicasting**,severalpacketsstartfromthesource.
  + Iftherearethreedestinations,forexample,thesourcesendsthreepackets,each with a different unicast destination address.
  + Theremaybemultiplecopiestravelingbetweentworouters

NEEDFORMULTICAST

Withoutsupportformulticast

* + Asourceneedstosendaseparate packetwith theidentical datatoeach member of the group
  + SourceneedstokeeptrackoftheIPaddressofeachmemberinthe group

UsingIPmulticast

* + Sendinghostdoesnotsendmultiplecopiesofthepacket
  + Ahostsendsasinglecopyofthepacketaddressedtothegroup’smulticast address
  + Thesending hostdoesnotneedtoknowtheindividualunicastIPaddressof each member

TYPESOFMULTICASTING

* + ***Source-Specific Multicast*** - In *source-specific* multicast (one-to-many model), receiverspecifiesmulticastgroupandsenderfromwhichitisinterestedto receive packets. Example: Internet radio broadcasts.
  + ***AnySourceMulticast*** -Supplements*anysource*multicast(many-to-many model).

MULTICASTAPPLICATIONS

* + - AccesstoDistributedDatabases
    - InformationDissemination
    - Teleconferencing.
    - DistanceLearning

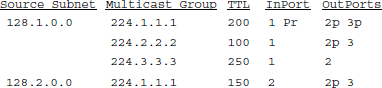
### MULTICASTROUTING

* + - To support multicast, a router must additionally have multicast forwarding tables that indicate, based on multicast address, which links to use to forward the multicast packet.
    - Unicastforwardingtablescollectivelyspecifyasetofpaths.
    - Multicastforwardingtablescollectivelyspecifyasetoftrees-Multicast distribution trees.
    - Multicastroutingistheprocessbywhichmulticastdistributiontreesare determined.
    - Tosupportmulticasting,routers*additionally*buildmulticastforwarding tables.
    - Multicastforwardingtableisatreestructure,knownas***multicast distribution trees*.**
    - Internetmulticastisimplementedonphysicalnetworksthatsupport

broadcastingby*extending*forwardingfunctions.

MULTICASTDISTRIBUTIONTREES

TherearetwotypesofMulticastDistributionTreesusedinmulticastrouting. They are

* **Source-BasedTree**:(DVMRP)
  + Foreachcombinationof(source,group),thereisashortestpathspanning tree.
  + Floodandprune
    - Sendmulticasttrafficeverywhere
    - Pruneedgesthatarenotactivelysubscribedtogroup
  + Link-state
    - Routersfloodgroupstheywouldliketoreceive
    - Computeshortest-pathtreesondemand
* **SharedTree**(PIM)
  + Singledistributedtreesharedamongallsources
  + Doesnotincludeitsowntopologydiscoverymechanism,but instead uses routing information supplied by other routing protocols
  + Specifyrendezvouspoint(RP)forgroup
  + SenderssendpacketstoRP,receiversjoinat RP
  + RPmulticaststoreceivers;Fix-uptreeforoptimization
  + ***Rendezvous-PointTree***:onerouteristhecenterofthegroup and

thereforetherootofthetree.

MULTICASTROUTINGPROTOCOLS

* Internet multicast is implemented on physical networks that support broadcasting by *extending forwarding functions.*
* Majormulticastroutingprotocolsare:
  1. Distance-VectorMulticastRoutingProtocol(DVMRP)
  2. ProtocolIndependentMulticast(PIM)

#### DistanceVectorMulticastRoutingProtocol

* + The DVMRP, is a routing protocol used to share information betweenrouterstofacilitatethetransportationofIPmulticastpacketsamong networks.
  + ItformedthebasisoftheInternet'shistoricmulticastbackbone.
  + Distancevectorroutingforunicastisextendedtosupportmulticastrouting.
  + Each routermaintainsa routing tableforall destinationthroughexchangeof distance vectors.
  + DVMRPisalsoknownas***flood-and-pruneprotocol****.*
  + DVMRPconsistsoftwomajorcomponents:
  + Aconventionaldistance-vectorroutingprotocol,likeRIP
  + Aprotocolfordetermininghowtoforwardmulticastpackets,basedonthe routing table
  + DVMRProuterforwardsapacket if
  + Thepacketarrivedfromthelinkusedtoreachthesourceofthepacket
  + Ifdownstreamlinkshavenotprunedthetree
  + DVMRPprotocolusesthe**basicpackettypes**asfollows:

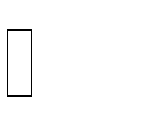


* + The**forwardingtable**ofDVMRPisasfollows:
* Multicastingisaddedtodistance-vectorroutinginfourstages.
  + Flooding
  + ReversePathForwarding(RPF)
  + ReversePathBroadcasting(RPB)
  + ReversePathMulticast(RPM)

Flooding

Routeronreceivingamulticastpacketfromsource*S*toaDestinationfrom NextHop, *forwards* the packet on all out-going links.

Packetisfloodedandloopedbackto*S*. The drawbacks are:



* Itfloodsanetwork,evenifithas*nomembers*forthatgroup.
* PacketsareforwardedbyeachrouterconnectedtoaLAN,i.e.,*duplicate flooding*

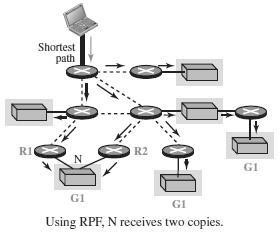
ReversePathForwarding(RPF)

RPF eliminates the looping problem in the flooding process. Onlyonecopyisforwardedandtheothercopiesarediscarded.



RPF forces the router to forward a multicast packet from one specific interface: theonewhichhascomethroughtheshortestpathfromthesourcetotherouter.

**Packetisfloodedbutnotloopedbackto*S.*

**

Reverse-PathBroadcasting(RPB)

RPBdoesnotmulticastthepacket,itbroadcastsit.



RPBcreatesashortestpathbroadcasttreefromthesourcetoeachdestination.

Itguaranteesthateachdestinationreceivesoneandonlyonecopyofthe packet.

Weneedtopreventeachnetwork from receivingmorethanonecopyofthe packet.

If a networkis connected to more than one router, it may receive a copy of the packet from each router.

OnerouteridentifiedasparentcalleddesignatedRouter(DR).



Only parent router*forwards* multicast packets from source*S to the attachednetwork.*

Whenarouterthatisnottheparentoftheattachednetworkreceivesamulticast packet, it simply drops the packet.



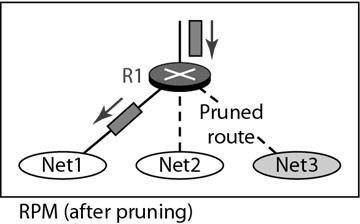
Reverse-PathMulticasting(RPM)

Toincreaseefficiency,themulticastpacketmustreachonly thosenetworks that have active members for that particular group.

RPM adds pruning and grafting to RPB to create a multicast shortest path tree that supports dynamic membership changes.

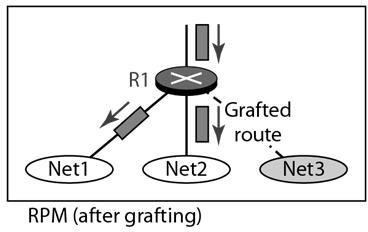
***Pruning:***

* + - Sentfromroutersreceivingmulticasttrafficforwhichtheyhavenoactive group members
    - “Prunes”thetreecreatedbyDVMRP
    - Stopsneedlessdatafrombeingsent



***Grafting:***

* Usedafterabranchhasbeenprunedback
* Sentbyarouterthathasahostthatjoinsamulticastgroup
* Goesfromroutertorouteruntilarouteractiveonthemulticastgroupisreached
* Sentforthefollowingcases
  + Anewhostmemberjoinsa group
  + Anewdependentrouterjoinsaprunedbranch
  + Adependentrouterrestartsonaprunedbranch



#### ProtocolIndependentMulticast(PIM)

PIMdividesmulticastroutingprobleminto*sparse*and*dense*mode. PIM sparse mode (PIM-SM) is widely used.



PIMdoesnotrelyonanytypeofunicastroutingprotocol,henceprotocol independent.

Routers explicitly join and leave multicast group using***Join and Prune messages***.

One of the router is designated as*rendezvous point* (RP) for each group in adomain to receive PIM messages.

Multicast forwarding*tree* is built as a result of routers sending Join messages to RP.

Twotypesoftreestobeconstructed:

* ***Sharedtree****-*usedbyallsenders
* ***Source-specific*tree**-usedonlybyaspecificsendinghost

The normal mode of operation creates the shared tree first, followed by one or more source-specific trees

**SharedTree**

WhenaroutersendsJoin messagefor group*G*toRP, itgoesthrougha setof routers.

Join message is *wildcarded* (\*), i.e., it is applicable to all senders. Routerscreatean*entry*(\*,*G*)initsforwardingtableforthesharedtree.



*Interface*onwhichtheJoinarrivedismarkedtoforwardpacketsforthat group.

*Forwards*Jointowardsrendezvousrouter RP.



Eventually,the message arrives at RP. Thus a shared tree with RP as*root* isformed.

Example

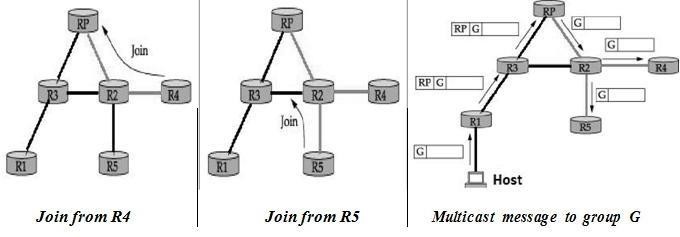
Router*R4*sendsJoinmessageforgroup*G*torendezvousrouterRP.



Join message is received by router*R2*. It makes an entry (\*,*G*) in its table and forwards the message to *RP*.

When*R5*sendsJoinmessageforgroup*G*,*R2*doesnotforwardstheJoin.It

*adds*anoutgoinginterfacetotheforwardingtablecreatedforthatgroup.



As routers send Join message for a group, branches are*added* to the tree, i.e., shared.

Multicastpacketssentfromhostsareforwardedto*designated*routerRP.

**Supposerouter*R1*,receivesamessagetogroup*G*. o*R1* has no state for group *G.*

* EncapsulatesthemulticastpacketinaRegistermessage.
* MulticastpacketistunneledalongthewaytoRP.

RPdecapsulatesthepacketandsendsmulticastpacketontothesharedtree, towards *R2*.

*R2*forwards the multicast packet to routers *R4*and *R5*that have members for group *G*.

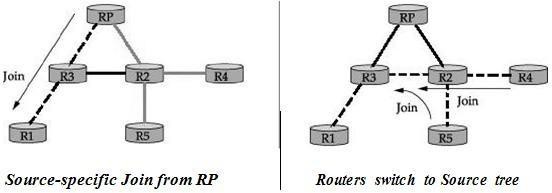
**Source-SpecificTree**

RPcanforcerouterstoknowabout group*G*,bysendingJoinmessagetothe sending host, so that tunneling can be avoided.

Intermediary routers create*sender-specific* entry (*S*,*G*) in their tables. Thus a source-specific route from *R1* to RP is formed.

If there is high rate of packets sent froma sender to a group*G*, then shared- tree is *replaced* by source*-*specific tree with sender as root.

Example

******

RendezvousrouterRPsendsaJoinmessagetothehostrouter*R1*. Router*R3*learnsaboutgroup*G*throughthemessagesentbyRP.

Router*R4*sendasource-specificJoinduetohighrateofpacketsfromsender. Router *R2* learns about group *G* through the message sent by *R4*.



Eventuallyasource-specifictreeisformedwith*R1*asroot.

AnalysisofPIM

Protocolindependentbecause,treeisbasedonJoinmessagesvia*shortest*path. Shared trees are more *scalable* than source-specific trees.



Source-specifictrees enable*efficient* routingthanshared trees.

**12.IPV6-NEXTGENERATIONIP**

* IPv6 was evolved to solve address space problem and offers rich set of services.
* SomehostsandrouterswillrunIPv4only,somewillrunIPv4andIPv6and some will run IPv6 only.

DRAWBACKSOFIPV4

* DespitesubnettingandCIDR,addressdepletionisstillalong-termproblem.
* Internetmustaccommodatereal-timeaudioandvideotransmissionthat requires minimum delay strategies and reservation of resources.
* Internet mustprovideencryptionandauthenticationofdataforsome applications

FEATURESOFIPV6

1. ***Betterheaderformat*-** IPv6usesanewheaderformatinwhichoptionsare separated from the base header and inserted,when needed, between the baseheader and the data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
2. ***Newoptions-***IPv6hasnewoptionstoallowforadditionalfunctionalities.
3. ***Allowanceforextension*-**IPv6isdesignedtoallowtheextensionofthe protocol if required by new technologies or applications.
4. ***Support forresource allocation*-** InIPv6, thetype-of-servicefieldhas been removed, but two new fields, traffic class and flow label, have been added toenablethe source to request special handling of the packet. This mechanismcan be used to support traffic such as real-time audio and video.

AdditionalFeatures:

* 1. Needtoaccommodatescalableroutingandaddressing
  2. Supportforreal-timeservices
  3. Securitysupport
  4. Autoconfiguration-

Theabilityofhoststoautomaticallyconfigurethemselveswithsuch information as their own IP address and domain name.

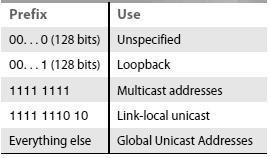
* 1. Enhancedroutingfunctionality,includingsupportformobilehosts
  2. Transitionfromipv4toipv6

ADDRESSSPACEALLOCATIONOFIPV6

IPv6providesa128-bitaddressspacetohandleupto3.4×1038nodes. IPv6 uses *classless* addressing, but classification is based on MSBs.



Theaddressspaceissubdividedinvariouswaysbasedontheleadingbits. The current assignment of prefixes is listed in Table



Anode maybeassignedan “IPv4-compatibleIPv6address”byzero-extending a 32-bit IPv4 addressto128 bits.

A node that is only capable of understanding IPv4 can be assigned an “IPv4- mapped IPv6 address” by prefixing the 32-bit IPv4 address with 2 bytes of all 1s and then zero-extending the result to 128 bits.

GLOBALUNICAST

Largechunks(87%)ofaddressspaceareleft*unassigned*forfutureuse.



IPv6definestwotypesof*local*addressesforprivatenetworks.

o***Linklocal***-enablesahosttoconstructanaddressthatneednotbe globally unique.

o***Sitelocal***-allowsvalidlocaladdressforuseinaisolatedsitewith several subnets.

*Reserved*addressesstartwithprefixofeight0's.

o***Unspecifiedaddress***isusedwhenahostdoesnotknowitsaddress o***Loopback address*** is used for testing purposes before connecting o***Compatible address*** is used when IPv6 hosts uses IPv4network

oM***appedaddress***isusedwhenaIPv6hostcommunicateswithaIPv4host IPv6 defines *anycast* address, assigned to a set of interfaces.



Packetwithanycastaddressisdeliveredtoonlyoneofthenearestinterface.

ADDRESSNOTATIONOFIPV6

StandardrepresentationofIPv6addressis ***x*:*x*:*x*:*x*:*x*:*x*:*x*:*x***where*x*isa 16-bit hexadecimal address separated by colon (:).

Forexample,

47CD**:**1234**:**4422**:**ACO2**:**0022**:**1234**:**A456**:**0124

IPv6addresswithcontiguous0bytescanbewrittencompactly. For example,

47CD**:**0000**:**0000**:**0000**:**0000**:**0000**:**A456**:**0124**→**47CD**::**A456**:**0124

IPv4addressismappedtoIPv6addressbyprefixingthe32-bitIPv4address with 2 bytes of 1s and then zero-extending the result to 128 bits.

Forexample,

128.96.33.81→::FFFF:128.96.33.81

ThisnotationiscalledasCIDRnotationorslashnotation.

ADDRESSAGGREGATIONOFIPV6

IPv6provides*aggregation*ofroutinginformationtoreducetheburdenon routers.

Aggregationisdonebyassigningprefixesat*continental*level.



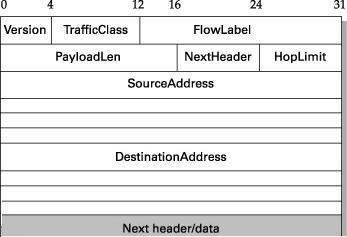
For *example*, if all addresses in Europe have a common prefix, then routers in othercontinentswouldneedoneroutingtableentryforallnetworksinEurope.



* + ***Prefix***-Alladdressesinthesamecontinenthaveacommonprefix
  + ***RegistryID***―identifiesthecontinent
  + ***ProviderID***―identifiestheproviderforInternetaccess,i.e.,ISP.
  + ***SubscriberID***―specifiesthesubscriberidentifier
  + ***SubnetID***―containssubnetofthesubscriber.
  + ***InterfaceID***―containslinklevelorphysicaladdress.

PACKETFORMATOFIPV6

IPv6baseheaderis40byteslong.



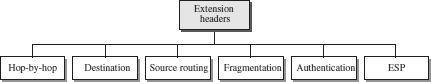
* ***Version***—specifiestheIPversion,i.e.,6.
* ***TrafficClass***—definespriorityofthepacketwithrespecttotraffic congestion.Itiseithercongestion-controlledornon-congestioncontrolled
* ***Flow Label*** — provides special handling for a particular flow of data. Routerhandles different flows with the help of a flow table.
* ***PayloadLen***—giveslengthofthepacket,excludingIPv6header.
* ***Next Heade***r — Options are specified as a header following IP header. NextHeader contains a pointer to optional headers.
* ***HopLimit***—GivestheTTLvalueofapacket.
* ***SourceAddress/DestinationAddress***—16-byteaddressesofsourceand destination host

ExtensionHeaders

ExtensionheaderprovidesgreaterfunctionalitytoIPv6. Baseheader maybefollowedbysixextensionheaders.



EachextensionheadercontainsaNextHeaderfieldtoidentifytheheader following it.



* + ***Hop-by-Hop***—sourcehostpassesinformationtoallroutersvisitedby the

packet

* + ***Destination***—sourcehostinformationispassedtothedestinationonly.
  + ***SourceRouting***—routinginformationprovidedbythesourcehost.
  + ***Fragmentation*** — In IPv6, only the source host can fragment. Source uses a pathMTUdiscoverytechniquetofindsmallest MTUonthepath.
  + ***Authentication****—*usedtovalidatethesenderandensuresdataintegrity.
  + ***ESP(EncryptedSecurityPayload)****—*providesconfidentialityagainst

eavesdropping.

ADVANCEDCAPABILITIESOFIPV6

**Auto Configuration**— Auto or stateless configuration of IP address to hosts without the need for a DHCP server, i.e., plug and play.

**AdvancedRouting**—Enhancedroutingsupportformobilehostsisprovided.



**AdditionalFunctions**―Enhancedroutingfunctionalitywithsupportfor mobile hosts.

**Security**― Encryption and authentication options provide confidentiality and integrity.

**Resource allocation**― Flow label enables the source to request special handling of real-time audio and video packets

ADVANTAGESOFIPV6

***Address space***― IPv6uses128-bit address whereas IPv4 uses 32-bit address. Hence IPv6 has huge address space whereas IPv4 faces address shortage problem.

***Header format*** ― Unlike IPv4, optional headers are separated from base headerinIPv6. Eachrouterthusneednotprocessunwantedaddition information.

***Extensible***―UnassignedIPv6addressescanaccommodateneedsoffuture technologies.

Dual-StackOperationandTunneling

Indual-stack,nodesrunbothIPv6andIPv4,usesVersionfieldtodecidewhich stack should process an arriving packet.

IPv6 packet is encapsulated with an IPv4 packet as it travels through an IPv4 network. This is known as tunneling and packet contains tunnel endpoint as its destination address.

NetworkAddressTranslation

NAT enables hosts on a network to use Internet with local addresses. Addresses reserved for internal use range from 172.16.0.0 to 172.31.255.255 Organization must have single connection to the Internet through a router that



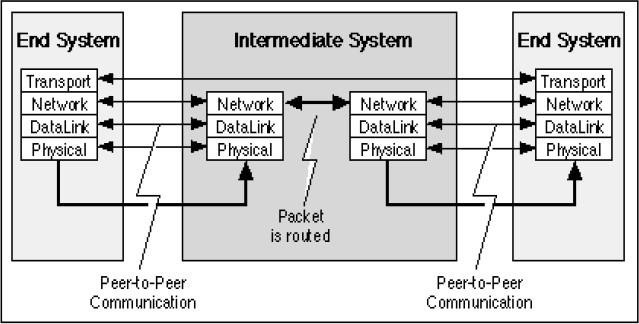
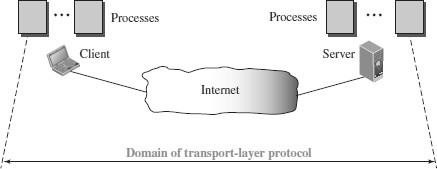
runstheNATsoftware.

**UNIT–IV:TRANSPORTLAYER**

**Introduction –TransportLayerProtocols–Services–PortNumbers– User Datagram Protocol – Transmission Control Protocol – SCTP.**

**1. INTRODUCTION**

* Thetransportlayeris thefourthlayerof theOSImodelandis thecoreof theInternet model.
* It responds to service requests from the session layer and issues service requests tothe network Layer.
* Thetransportlayerprovidestransparenttransferofdatabetweenhosts.
* Itprovidesend-to-endcontrolandinformationtransferwiththequalityofservice needed by the application program.
* Itisthefirsttrueend-to-endlayer,implementedinallEndSystems(ES).



### TRANSPORTLAYERFUNCTIONS/SERVICES

* Thetransportlayerislocatedbetweenthenetworklayerandtheapplicationlayer.
* The transport layer is responsible for providing services to the application layer; itreceives services from the network layer.
* Theservicesthatcanbeprovidedbythetransportlayer are

1. Process-to-ProcessCommunication
2. Addressing:PortNumbers
3. EncapsulationandDecapsulation
4. MultiplexingandDemultiplexing
5. FlowControl
6. ErrorControl
7. CongestionControl

#### Process-to-ProcessCommunication

* The Transport Layer is responsible for delivering data to the appropriate application process on the host computers.
* This involves multiplexing of data from different application processes, i.e. forming data packets, and adding source and destination port numbers in the header of each Transport Layer data packet.
* Together with the source and destination IP address, the port numbers constitutes a network socket, i.e. an identification address of the process-to-process communication.

#### Addressing:PortNumbers

* Portsaretheessentialwaystoaddressmultipleentitiesinthesamelocation.
* Using port addressing it is possible to use more than one network-based application at the same time.
* ThreetypesofPortnumbersareused:
  + ***Well-known ports*** *-* These are permanent port numbers. They rangebetween 0 to 1023.These port numbers are used by Server Process.
  + ***Registered ports -*** The ports ranging from1024 to 49,151 are not assigned or controlled.
  + ***Ephemeral ports (Dynamic Ports) –*** These are temporary port numbers. They range between 49152–65535.These port numbers are used by Client Process**.**

#### EncapsulationandDecapsulation

* To send a message from one process to another, the transport-layer protocol encapsulates and decapsulates messages.
* Encapsulation happens at the sender site. The transport layer receives the data and adds the transport-layer header.
* Decapsulation happens at the receiver site. When the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer.

#### MultiplexingandDemultiplexing

* Wheneveranentityacceptsitemsfrommorethanonesource,thisisreferredtoas

***multiplexing***(manytoone).

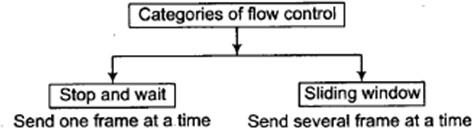
* Wheneveranentitydeliversitemstomorethanonesource,thisisreferredtoas

***demultiplexing***(onetomany).

* Thetransportlayeratthesourceperformsmultiplexing
* Thetransportlayeratthedestinationperformsdemultiplexing

#### FlowControl

* Flow Control is the process of managing the rate of data transmission between twonodes to prevent a fast sender from overwhelming a slow receiver.
* Itprovidesa mechanismforthereceivertocontrolthetransmissionspeed,sothatthe receiving node is not overwhelmed with data from transmitting node.

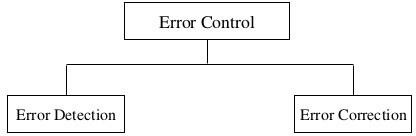


#### ErrorControl

* Errorcontrolatthetransportlayerisresponsiblefor

1. Detectinganddiscardingcorruptedpackets.
2. Keepingtrackoflostanddiscardedpacketsandresendingthem.
3. Recognizingduplicatepacketsanddiscardingthem.
4. Bufferingout-of-orderpacketsuntilthemissingpacketsarrive.

* ErrorControlinvolvesErrorDetectionandErrorCorrection

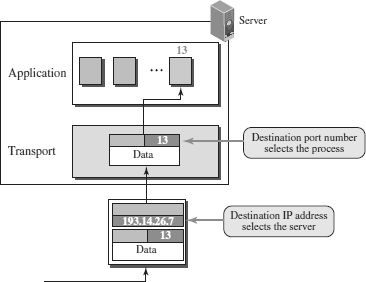


#### CongestionControl

* Congestion in a network may occur if the *load* on the network (the number of packetssenttothenetwork)isgreaterthanthe *capacity*ofthenetwork(thenumber of packets a network can handle).
* Congestioncontrolreferstothemechanismsandtechniquesthatcontrolthe congestion and keep the load below the capacity.
* CongestionControlreferstotechniquesandmechanismsthatcaneitherprevent congestion, before it happens, or remove congestion, after it has happened
* Congestioncontrolmechanismsaredividedintotwocategories,

1. Openloop-preventthecongestionbeforeithappens.
2. Closedloop-removethecongestionafterithappens.

**2. PORTNUMBERS**

* Atransport-layerprotocolusuallyhasseveralresponsibilities.
* Oneistocreateaprocess-to-processcommunication.
* Processesareprogramsthatrunonhosts.Itcouldbeeither*server*or*client*.
* Aprocessonthelocalhost,calleda *client,* needsservicesfromaprocessusually on the remote host, called a *server.*
* Processesareassignedaunique16-bit*portnumber*onthathost.
* Portnumbersprovideend-to-endaddressesatthetransportlayer
* Theyalsoprovidemultiplexinganddemultiplexingatthislayer.
* Theportnumbersareintegersbetween0and65,535.

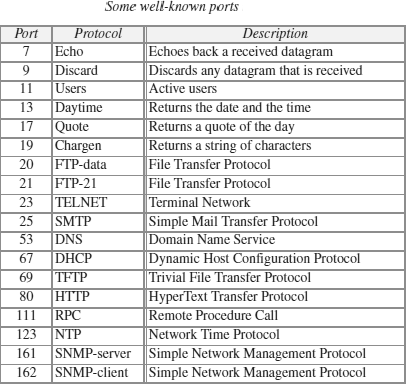
ICANN(InternetCorporationforAssignedNamesandNumbers) hasdividedtheport numbers into three ranges:

* + **Well-knownports**
  + **Registered**
  + **Ephemeralports(DynamicPorts)**



WELL-KNOWNPORTS

* Thesearepermanentportnumbersusedbytheservers.
* Theyrangebetween 0to1023.
* Thisportnumbercannotbechosenrandomly.
* Theseportnumbersareuniversalportnumbersforservers.
* Every client process knows the well-known port number of the corresponding server process.
* For example, while thedaytime clientprocess,awell-known clientprogram, can useanephemeral(temporary)portnumber, 52,000,toidentifyitself,thedaytime server process must use the well-known (permanent) port number 13.



EPHEMERALPORTS(DYNAMICPORTS)

* Theclientprogramdefinesitselfwithaportnumber,calledthe***ephemeralport number.***
* The word *ephemeral* means “short-lived”andis used because the life of a client isnormally short.
* Anephemeralportnumberisrecommendedtobegreaterthan1023.
* Theseportnumberrangesfrom49,152to65,535.
* They are neither controlled nor registered. They can be used as temporary or private port numbers.

REGISTEREDPORTS

* Theportsrangingfrom1024to49,151arenotassignedorcontrolled.

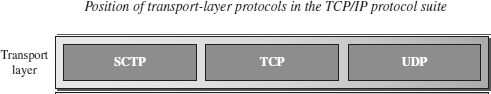
**3. TRANSPORTLAYERPROTOCOLS**

* ThreeprotocolsareassociatedwiththeTransportlayer.
* Theyare
  1. **UDP–UserDatagramProtocol**
  2. **TCP–TransmissionControlProtocol**
  3. **SCTP-StreamControlTransmissionProtocol**
* Eachprotocolprovidesadifferenttypeofserviceandshouldbeusedappropriately.

**UDP -** UDP is an unreliable connectionless transport-layer protocol used for its simplicity and efficiency in applications where error control can be provided by the application-layer process.

**TCP -** TCP is a reliable connection-oriented protocol that can be used in any application where reliability is important.

**SCTP -** SCTP is a new transport-layer protocol designed to combine some features of UDP and TCP in an effort to create a better protocol for multimedia communication.



## 4. USERDATAGRAMPROTOCOL(UDP)

* UserDatagramProtocol(UDP)isaconnectionless,unreliabletransportprotocol.
* UDPaddsprocess-to-processcommunicationtobest-effortserviceprovidedbyIP.
* UDPisaverysimpleprotocolusingaminimumofoverhead.
* UDPisasimpledemultiplexer,which allowsmultipleprocessesoneachhostto communicate.
* UDPdoesnotprovideflowcontrol,reliableorordered delivery.
* UDPcanbeusedtosendsmallmessagewhere reliabilityisnotexpected.
* Sendingasmall messageusingUDPtakesmuchlessinteractionbetweenthesender and receiver.
* UDP allow processes toindirectly identify each other usingan abstract locatorcalled port or mailbox

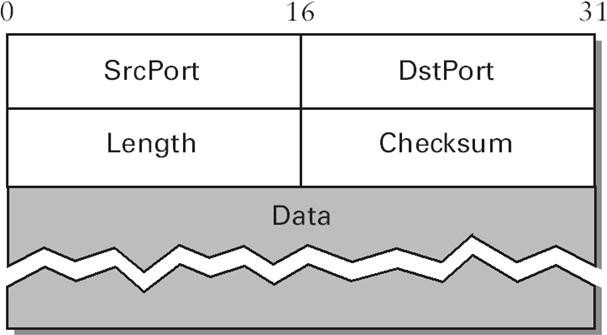
### UDPPORTS

* Processes(server/client)areidentifiedbyanabstractlocatorknownasport.
* Serveracceptsmessageat*wellknownport*.
* Somewell-knownUDPportsare7–Echo,53–DNS,111–RPC,161–SNMP,etc.
* <*port*, *host*>pairisusedaskeyfor demultiplexing.
* Portsareimplementedasa*messagequeue*.
* Whenamessagearrives,UDP*appends*ittoendofthequeue.
* Whenqueueis*full*,themessageisdiscarded.
* Whenamessageis*read*,itisremovedfromthequeue.
* When an applicationprocess wants toreceiveamessage,one isremoved from the front of the queue.
* Ifthequeueisempty,theprocessblocksuntilamessagebecomesavailable.



### UDPDATAGRAM(PACKET)FORMAT

* UDPpacketsareknownasuser*datagrams*.
* These***userdatagrams,*** haveafixed-sizeheaderof8bytesmadeoffourfields,each of 2 bytes (16 bits).



#### SourcePortNumber

* Portnumberusedbyprocessonsourcehostwith16bitslong.
* If the source host is client (sendingrequest) then the port number is an temporary one requested by the process and chosen by UDP.
* Ifthesourceisserver(sendingresponse)thenitiswellknownportnumber.

#### DestinationPortNumber

* PortnumberusedbyprocessonDestinationhostwith16bitslong.
* Ifthedestinationhostistheserver(aclientsendingrequest)thenthe port number is a well known port number.
* Ifthedestinationhostisclient(aserver sendingresponse)thenportnumber is an temporary one copied by server from the request packet.

#### Length

* ThisfielddenotesthetotallengthoftheUDPPacket(Headerplusdata)
* ThetotallengthofanyUDPdatagramcanbefrom0to65,535bytes.

#### Checksum

* UDP computes its checksum over the UDP header, the contents of the messagebody, and something called the pseudoheader.
* The pseudoheader consists of three fields from the IP header—protocol number, source IP address, destination IP address plus the UDP length field.

#### Data

* Datafielddefinesthaactualpayloadtobe transmitted.
* Itssizeisvariable**.**

### UDPSERVICES

#### Process-to-ProcessCommunication

* + UDP provides process-to-process communication using socket addresses**,** a combination of IP addresses and port numbers.

#### ConnectionlessServices

* + UDPprovidesaconnectionlessservice.
  + Thereisnoconnectionestablishmentandnoconnectiontermination.
  + EachuserdatagramsentbyUDPisanindependentdatagram.
  + Thereisnorelationshipbetweenthedifferentuserdatagramseveniftheyare
  + comingfromthesamesourceprocessandgoingtothesamedestinationprogram.
  + Theuserdatagramsarenotnumbered.
  + Eachuserdatagramcantravelonadifferentpath.

#### FlowControl

* + UDPisaverysimpleprotocol.
  + Thereisnoflowcontrol,andhencenowindow mechanism.
  + Thereceivermayoverflowwithincomingmessages.
  + ThelackofflowcontrolmeansthattheprocessusingUDPshouldprovideforthis service, if needed.

#### ErrorControl

* + ThereisnoerrorcontrolmechanisminUDPexceptforthechecksum.
  + Thismeansthatthesenderdoesnotknowifamessagehasbeenlostorduplicated.
  + Whenthereceiverdetectsanerrorthroughthechecksum,theuserdatagramissilently discarded.
  + The lack of error control means that the process using UDP should provide for thisservice, if needed.

#### Checksum

* + UDP checksumcalculation includes three sections: a pseudoheader, theUDP header, and the data coming from the application layer.
  + Thepseudoheaderisthepartoftheheaderinwhichtheuserdatagramistobe encapsulated with some fields filled with 0s.

OptionalInclusionofChecksum

* + - ThesenderofaUDPpacketcanchoosenottocalculatethechecksum.
    - Inthiscase,thechecksumfieldisfilledwithall0sbeforebeingsent.
    - In the situation where the sender decides to calculate the checksum,butithappensthattheresultisall0s,thechecksumischangedtoall1s before the packet is sent.
    - Inotherwords,thesendercomplementsthesumtwotimes.

#### CongestionControl

* + SinceUDPisaconnectionlessprotocol,itdoesnotprovidecongestioncontrol.
  + UDPassumesthatthepacketssentaresmallandsporadic(occasionallyoratirregular intervals) and cannot create congestion in the network.
  + This assumption may or may not be true, when UDP is used for interactive real-time transfer of audio and video.

#### EncapsulationandDecapsulation

* + Tosendamessagefromoneprocessto another,theUDPprotocolencapsulatesand decapsulates messages.

#### Queuing

* + InUDP,queuesareassociatedwithports.
  + Attheclientsite,whenaprocessstarts,itrequestsaportnumberfromtheoperating system.
  + Someimplementationscreatebothanincomingandanoutgoingqueueassociated with each process.
  + Otherimplementationscreateonlyanincomingqueueassociatedwitheachprocess.

#### MultiplexingandDemultiplexing

* + Inahostrunningatransport protocolsuite,thereisonlyoneUDPbutpossibly several processes that may want to use the services of UDP.
  + Tohandlethissituation,UDPmultiplexesanddemultiplexes.

### APPLICATIONSOFUDP

* + UDPisusedformanagementprocessessuchasSNMP.
  + UDPisusedforrouteupdatingprotocolssuchasRIP.
  + UDPisasuitabletransportprotocolformulticasting.Multicastingcapabilityis embedded in the UDP software
  + UDP is suitable for a process with internal flow and error control mechanisms such as Trivial File Transfer Protocol (TFTP).
  + UDP is suitable for a process that requires simple request-response communicationwith little concern for flow and error control.
  + UDPisnormallyusedforinteractivereal-timeapplicationsthatcannottolerate uneven delay between sections of a received message.

## 5. TRANSMISSIONCONTROLPROTOCOL(TCP)

* TCPisareliable,connection-oriented,byte-streamprotocol.
* TCP guarantees the reliable, in-order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.
* TCP includes a flow-control mechanismfor each of thesebyte streams that allow the receiver to limit how much data the sender can transmit at a given time.
* TCPsupportsademultiplexingmechanismthatallowsmultipleapplicationprograms on any given host to simultaneously carry on a conversation with their peers.
* TCP also implements congestion-control mechanism. The idea of this mechanism is to prevent sender from overloading the network.
* Flowcontrolisanendtoendissue,whereascongestioncontrolisconcernedwith how host and network interact.

### TCPSERVICES

Process-to-ProcessCommunication

* + TCPprovidesprocess-to-processcommunicationusingportnumbers.

StreamDeliveryService

* + TCPisastream-orientedprotocol.
  + TCP allowsthe sending processtodeliverdataas astream of bytesand allowsthe receiving process to obtain data as a stream of bytes.
  + TCP creates an environment in which the two processes seem to be connected by an imaginary “tube” that carries their bytes across the Internet.
  + The sendingprocess produces (writes to) the streamand the receivingprocess consumes (reads from) it.

11



Full-DuplexCommunication

* + TCPoffersfull-duplexservice,wheredatacanflowinboth directionsatthesame time.
  + EachTCPendpointthenhasitsownsendingandreceivingbuffer,andsegments move in both directions.

MultiplexingandDemultiplexing

TCPperformsmultiplexingatthesenderanddemultiplexingatthereceiver.

Connection-OrientedService

* + TCPisaconnection-orientedprotocol.
  + Aconnectionneedstobeestablishedforeachpairofprocesses.
  + WhenaprocessatsiteAwantstosendtoandreceivedatafromanother process at site B, the following three phases occur:

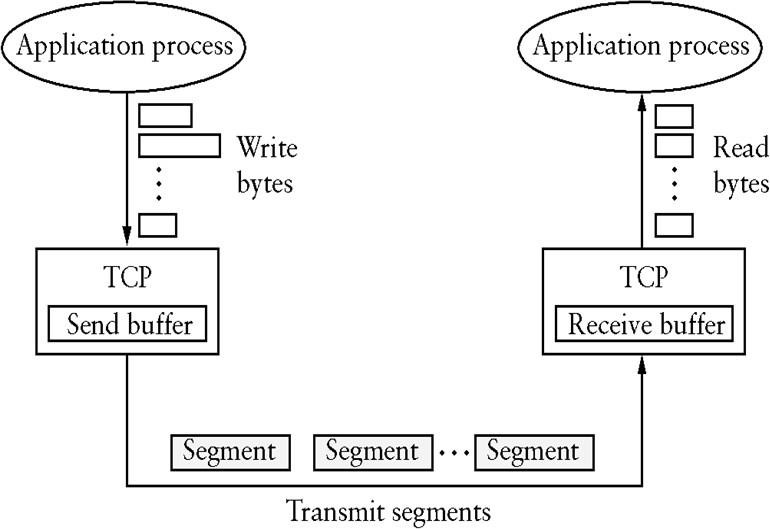
1. ThetwoTCP’sestablishalogicalconnectionbetweenthem.
2. Dataareexchangedinbothdirections.
3. Theconnectionisterminated.

ReliableService

* + TCPisareliabletransportprotocol.
  + Itusesanacknowledgment mechanismtocheckthesafeandsoundarrivalofdata.

### TCPSEGMENT

* + ApacketinTCPiscalledasegment.
  + DataunitexchangedbetweenTCPpeersarecalled***segments*.**
  + ATCPsegmentencapsulatesthedatareceivedfromtheapplicationlayer.
  + TheTCPsegmentisencapsulatedinanIPdatagram,whichinturnisencapsulatedin a frame at the data-link layer.



**annauniversityedu.blogspot.com**

* + TCPisabyte-orientedprotocol, which means thatthesenderwritesbytesintoaTCP connection and the receiver reads bytes out of the TCP connection.
  + TCPdoesnot,itself,transmitindividualbytesovertheInternet.
  + TCPonthesourcehostbuffersenoughbytesfromthesendingprocesstofilla reasonably sized packet and then sends this packet to its peer on thedestination host.
  + TCPonthedestinationhostthenemptiesthecontentsofthepacketintoareceive buffer, and the receiving process reads from this buffer at its leisure.
  + TCPconnectionsupportsbytestreamsflowinginbothdirections.
  + ThepacketsexchangedbetweenTCPpeersarecalledsegments,sinceeachone carries a segment of the byte stream.

### TCPPACKETFORMAT

* + EachTCPsegmentcontainstheheaderplusthedata.
  + Thesegmentconsistsofaheaderof20to60bytes,followedbydatafromthe application program.
  + Theheaderis20bytesiftherearenooptionsandupto60bytesifitcontains options.



**SrcPort and DstPort**―port number of source and destination process. **SequenceNum**―containssequencenumber,i.e.firstbyteofdatasegment. **Acknowledgment**― byte number of segment, the receiver expects next.

**HdrLen**―LengthofTCPheaderas4-bytewords.

**Flags**― contains***six***controlbitsknownasflags.

* **URG**—segmentcontainsurgentdata.
* **ACK**—valueofacknowledgmentfieldisvalid.
* **PUSH**—senderhasinvokedthepushoperation.
* **RESET**—receiverwantstoaborttheconnection.
* **SYN**—synchronizesequencenumbersduringconnectionestablishment.
* **FIN**—terminatestheTCPconnection.

12

**AdvertisedWindow**―definesreceiver’swindowsizeandactsasflowcontrol.

**Checksum**―ItiscomputedoverTCPheader,Data,andpseudoheadercontainingIPfields

(Length,SourceAddr&DestinationAddr).

**UrgPtr**―usedwhenthesegmentcontainsurgentdata.Itdefinesavaluethat mustbe added to the sequence number.

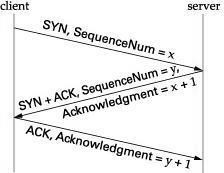
**Options-**Therecanbeupto40bytesofoptionalinformationin theTCPheader.

### TCPCONNECTIONMANAGEMENT

* + TCPisconnection-oriented.
  + Aconnection-orientedtransportprotocolestablishesalogicalpathbetweenthe source and destination.
  + Allofthesegmentsbelongingtoamessagearethensentoverthislogicalpath.
  + In TCP, connection-oriented transmission requires three phases: ConnectionEstablishment,DataTransferandConnectionTermination.

#### ConnectionEstablishment

* While openinga TCP connection the two nodes(client and server) want to agree on a set of parameters.
* Theparameters arethestartingsequencenumbersthatistobeusedfortheir respective byte streams.
* ConnectionestablishmentinTCPisa*three-wayhandshaking*.



1. ClientsendsaSYNsegmenttotheservercontainingitsinitialsequencenumber(Flags

**=**SYN,SequenceNum**=***x*)

1. Serverrespondswithasegmentthatacknowledgesclient’ssegmentandspecifiesits initial sequence number (Flags **=** SYN **+** ACK, ACK **=** *x* **+** 1 SequenceNum **=** *y*).
2. Finally,clientrespondswithasegmentthatacknowledgesserver’ssequencenumber

(Flags**=**ACK,ACK**=***y***+**1).

13

* + The reason that each side acknowledges a sequence number that is one larger than the one sent is that the Acknowledgment field actually identifies the “next sequence number expected,”
  + A timer is scheduled for each of the first two segments, and if the expected response is not received, the segment is retransmitted.

#### DataTransfer

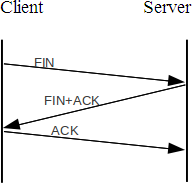
* + Afterconnectionisestablished,bidirectionaldatatransfercantakeplace.
  + Theclientandservercansenddataandacknowledgmentsinbothdirections.
  + Thedatatravelinginthesamedirectionasanacknowledgmentarecarriedonthe same segment.
  + Theacknowledgmentispiggybackedwiththedata.

#### ConnectionTermination

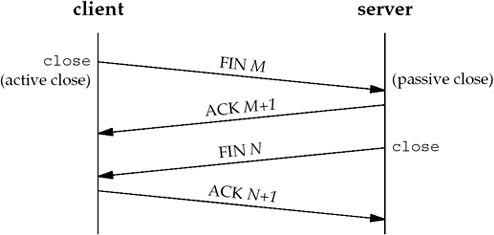
* Connectionterminationorteardowncanbedoneintwoways:

Three-wayCloseandHalf-Close

***Three-wayClose****—*Bothclientandserverclose*simultaneously.*

* + ClientsendsaFINsegment.
  + TheFINsegmentcanincludelast chunk of data.
  + ServerrespondswithFIN+ACK segment to inform its closing.
  + Finally,clientsendsanACK segment

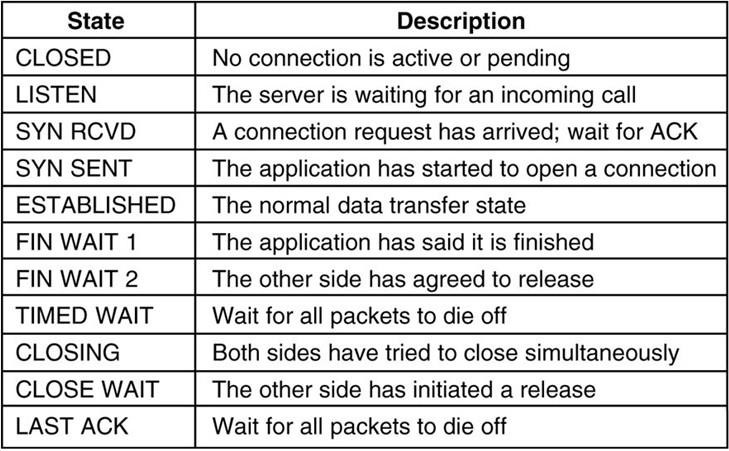
***Half*-*Close****—*Clientstopssendingbutreceivesdata.

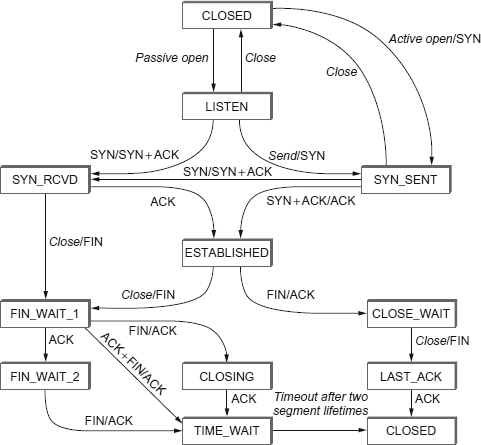
* + Client half-closes the connection by sending a FIN segment.
  + ServersendsanACKsegment.
  + Data transfer from client to the server *stops*.
  + After sending all data, server sends FIN segment to client, which is acknowledged by the client.

14

STATETRANSITIONDIAGRAM

* To keep track of all the different events happening during connection establishment, connectiontermination,anddatatransfer,TCPisspecifiedasthefinitestatemachine (FSM).
* Thetransitionfromonestatetoanotherisshownusingdirectedlines.
* Statesinvolvedinopeningandclosingaconnectionisshownaboveandbelow ESTABLISHED state respectively.
* StatesInvolvedinTCP:





15

OpeningaTCPConnection

1. Serverinvokesa*passive*openonTCP,whichcausesTCPtomovetoLISTENstate
2. Clientdoesan*active*open,whichcausesitsTCPtosendaSYNsegmenttotheserver and move to SYN\_SENT state.
3. WhenSYNsegmentarrivesattheserver,itmovestoSYN\_RCVDstateand*responds*

withaSYN**+**ACKsegment.

1. Arrival of SYN **+** ACK segment causes the client to move to ESTABLISHED stateand sends an ACK to the server.
2. WhenACKarrives,theserverfinallymovestoESTABLISHEDstate.

ClosingaTCPConnection

Client/Servercanindependentlycloseitshalfoftheconnectionorsimultaneously.

TransitionsfromESTABLISHEDtoCLOSEDstateare:

Onesidecloses:

ESTABLISHED**→**FIN\_WAIT\_1**→**FIN\_WAIT\_2 **→**TIME\_WAIT**→**CLOSED

Othersidecloses:

ESTABLISHED**→**CLOSE\_WAIT**→**LAST\_ACK**→**CLOSED

Simultaneousclose:

ESTABLISHED**→**FIN\_WAIT\_1**→**CLOSING**→**TIME\_WAIT**→**CLOSED

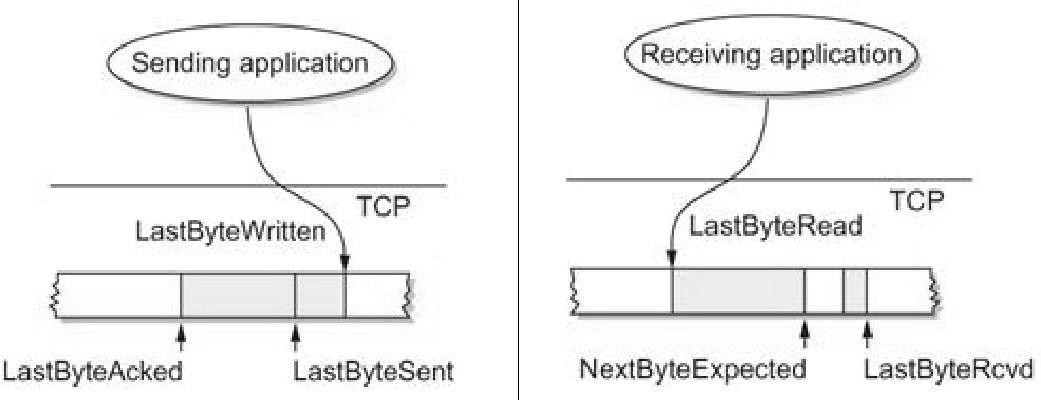
### TCPFLOW CONTROL

* TCPusesavariantofslidingwindowknownasadaptiveflowcontrolthat:

oguarantees*reliable*deliveryofdata

oensures*ordered*deliveryofdata

oenforces*flowcontrol*atthesender

* ReceiveradvertisesitswindowsizetothesenderusingAdvertisedWindowfield.
* Senderthuscannothave*unacknowledged*datagreaterthanAdvertisedWindow.

# annauniversityedu.blogspot.com

16

#### SendBuffer

* SendingTCPmaintains*sendbuffer*whichcontains3segments
  1. acknowledgeddata
  2. unacknowledgeddata
  3. datatobe transmitted.
* Sendbuffer maintainsthree*pointers*

(1) LastByteAcked, (2) LastByteSent, and (3)LastByteWritten such that:

LastByteAcked≤LastByteSent≤LastByteWritten

* Abytecanbesentonly*after*beingwrittenandonlyasentbyte*canbe*

acknowledged.

* Bytestothe*left*ofLastByteAckedarenotkeptasithadbeenacknowledged.

#### ReceiveBuffer

* ReceivingTCPmaintains*receive*buffertoholddataevenifitarrivesout-of-order.
* Receivebuffermaintainsthree*pointers*namely

(1) LastByteRead,(2)NextByteExpected,and(3)LastByteRcvd such that:

LastByteRead≤ NextByteExpected≤LastByteRcvd+1

* Abyte*cannot*bereaduntilthatbyteandallprecedingbyteshavebeenreceived.
* Ifdataisreceived*inorder*,thenNextByteExpected**=**LastByteRcvd**+**1
* Bytestothe*left*ofLastByteReadarenotbuffered,sinceitisreadbytheapplication.

#### FlowControlinTCP

* Sizeof*send*and*receive*bufferis*MaxSendBuffer*and*MaxRcvBuffer*respectively.
* SendingTCPprevents*overflowing*ofsendbufferbymaintaining

LastByteWritten−LastByteAcked≤MaxSendBuffer

* ReceivingTCPavoids*overflowing*itsreceivebufferbymaintaining

LastByteRcvd−LastByteRead≤MaxRcvBuffer

* Receiver*throttles*thesenderbyhavingAdvertisedWindowbasedon*free*space

availableforbuffering.

AdvertisedWindow=MaxRcvBuffer−((NextByteExpected−1)–LastByteRead)

* SendingTCP*adheres*toAdvertisedWindowbycomputingEffectiveWindowthat

*limits*howmuchdataitshouldsend.

EffectiveWindow=AdvertisedWindow−(LastByteSent−LastByteAcked)

* Whendataarrives,LastByteRcvdmovestoitsrightandAdvertisedWindowshrinks.
* Receiveracknowledgesonly,ifprecedingbyteshavearrived.
* AdvertisedWindow*expands*whendatais*read*bytheapplication. oIf data is read as *fast* as it arrives then

AdvertisedWindow=MaxRcvBuffer

o Ifdataisread*slowly*,iteventuallyleadstoaAdvertisedWindowofsize0.

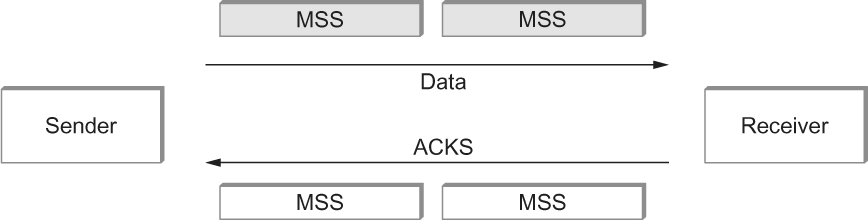
* AdvertisedWindowfieldisdesignedtoallowsendertokeepthepipe*full*.

### TCPTRANSMISSION

* TCPhasthreemechanismtotriggerthetransmissionofasegment.
* Theyare
* MaximumSegmentSize(MSS)-SillyWindowSyndrome
* Timeout-Nagle’sAlgorithm

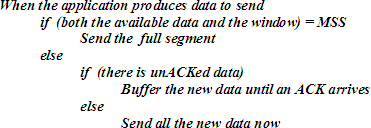
#### SillyWindowSyndrome

* Wheneitherthesendingapplicationprogramcreatesdataslowly orthereceiving application program consumes data slowly, or both, problems arise.
* Anyofthesesituationsresultsinthesendingofdatainverysmallsegments,which reduces the efficiency of the operation.
* Thisproblemiscalledthesillywindowsyndrome.
* The sending TCP may create a silly window syndrome if it is serving an application program that creates data slowly, for example, 1 byte at a time.
* Theapplicationprogramwrites1byteatatimeintothebufferofthesendingTCP.
* Theresultisalotof1-bytesegmentsthataretravelingthroughaninternet.
* ThesolutionistopreventthesendingTCPfromsendingthedatabytebybyte.
* ThesendingTCPmustbeforcedtowaitandcollectdatatosendinalargerblock.



#### Nagle’sAlgorithm

* If there is data to send but is less than MSS, then we may want to wait some amount of time before sending the available data
* Ifwewaittoolong,thenitmaydelaytheprocess.
* Ifwedon’twaitlongenough,itmayendupsendingsmallsegmentsresultingin Silly Window Syndrome.
* Thesolutionistointroduceatimerandtotransmitwhenthetimerexpires
* Nagleintroducedanalgorithmforsolvingthisproblem



### TCPCONGESTIONCONTROL

* Congestionoccursifload(numberofpacketssent)isgreaterthancapacityofthe network (number of packets a network can handle).
* Whenloadislessthannetworkcapacity,throughputincreasesproportionally.
* When load exceeds capacity,queues become full and the routersdiscard some packets and throughput declines sharply.
* Whentoomanypacketsarecontendingforthesamelink
* Thequeueoverflows
* Packetsgetdropped
* Networkis congested
* Network should provide a congestion control mechanism to deal with such a situation.
* TCPmaintainsavariablecalled*CongestionWindow*foreach*connection*.
* TCPCongestionControlmechanismsare:

1. AdditiveIncrease/MultiplicativeDecrease(AIMD)
2. SlowStart
3. FastRetransmitandFastRecovery

#### AdditiveIncrease/MultiplicativeDecrease(AIMD)

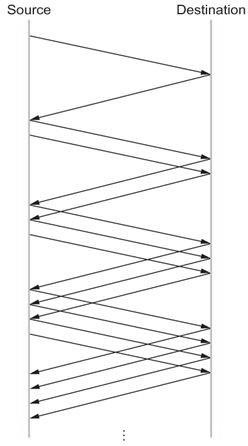
* TCPsource*initializes*CongestionWindowbasedoncongestionlevelinthenetwork.
* Source*increases*CongestionWindowwhenlevelofcongestiongoesdownand

*decreases*thesamewhenlevelofcongestiongoesup.

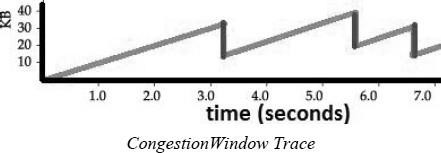
* TCPinterprets*timeouts*asasignofcongestionandreducestherateoftransmission.
* On timeout, source reduces its CongestionWindow by half, i.e., *multiplicative decrease*.Forexample,ifCongestionWindow =16packets,aftertimeoutitis8.
* ValueofCongestionWindowisneverlessthanmaximumsegmentsize(MSS).
* WhenACK arrives CongestionWindow is *incremented* marginally, i.e., *additive increase.*

Increment=MSS×(MSS/CongestionWindow) CongestionWindow += Increment

* For*example*,whenACKarrivesfor1packet,2packetsaresent. WhenACKforboth packets arrive, 3 packets are sent and so on.
* CongestionWindowincreasesanddecreasesthroughout*lifetime*oftheconnection.



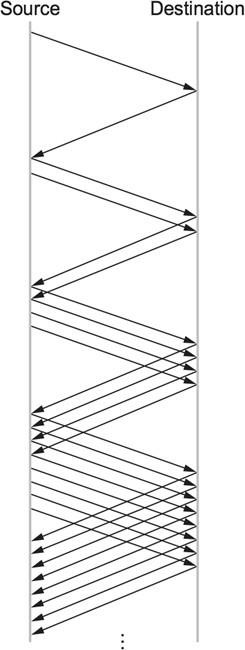
* When CongestionWindow is plotted as a function of time, a *saw-tooth* pattern results.

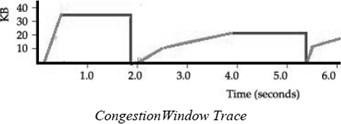


#### SlowStart

* SlowstartisusedtoincreaseCongestionWindow*exponentially*fromacoldstart.
* SourceTCP*initializes*CongestionWindowtoonepacket.
* TCP*doubles*thenumberofpacketssenteveryRTTonsuccessfultransmission.
* WhenACKarrivesforfirstpacketTCPadds1packettoCongestionWindowand sends two packets.
* WhentwoACKs arrive,TCPincrements CongestionWindow by2packetsandsends four packets and so on.
* Instead of sendingentire permissible packets at once (bursty traffic),packets are sent in a phased manner, i.e., *slow start*.
* Initially TCP has no idea about congestion, henceforth it increases CongestionWindow rapidly until there is a timeout. On timeout:

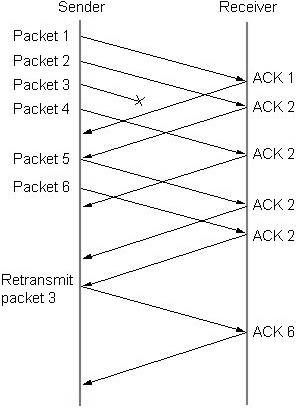
CongestionThreshold=CongestionWindow/2 CongestionWindow = 1

* SlowstartisrepeateduntilCongestionWindowreachesCongestionThresholdand thereafter 1 packet per RTT.
* Thecongestionwindowtracewilllooklike

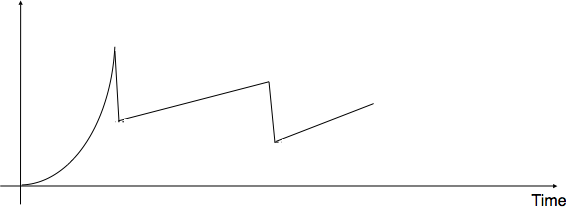


#### FastRetransmitAndFastRecovery

* TCP timeouts led to long periods of time during which the connection went dead while waiting for a timer to expire.
* Fast retransmit is a heuristic approach that *triggers* retransmission of a dropped packet sooner than the regular timeout mechanism. It *does not* replace regular timeouts.
* When a packet arrives out of order, receiving TCP resends thesameacknowledgment (*duplicate ACK*) it sent last time.
* When *three duplicate* ACK arrives at the sender, it infers that corresponding packet may be lost due to congestion and retransmits that packet. This is called ***fast retransmit*** before regular timeout.
* When packet loss is detectedusingfast retransmit, the slow startphase isreplacedby additive increase, multiplicative decrease method. This is known as ***fast recovery***.
* Instead of setting CongestionWindow to one packet, this method uses the ACKs that are still in pipe to clock the sending of packets.
* Slow start is only used at the beginningof a connection and after *regular* timeout. At other times, it follows a pure AIMD pattern.



* Forexample,packets1and2arereceivedwhereaspacket3getslost.
* ReceiversendsaduplicateACKforpacket2whenpacket4arrives.
* Senderreceives3duplicateACKsaftersendingpacket6retransmitspacket3.
* Whenpacket3isreceived,receiversendscumulativeACKuptopacket6.
* Thecongestionwindowtracewilllooklike



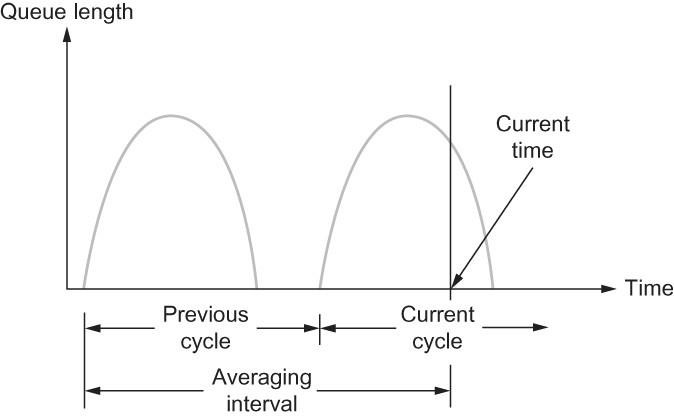
### TCP CONGESTION AVOIDANCE

* Congestionavoidancemechanisms*prevent*congestionbeforeitactuallyoccurs.
* Thesemechanismspredictwhen congestionisabouttohappenandthentoreducethe rate at which hosts send data just before packets start being discarded.
* TCP*creates*lossofpacketsinordertodeterminebandwidthoftheconnection.
* Routers*help*theendnodesbyintimatingwhencongestionislikelytooccur.
* Congestion-avoidancemechanismsare:
* DECbit-DestinationExperiencingCongestionBit
* RED-RandomEarlyDetection

#### DecBit-DestinationExperiencingCongestionBit

* ThefirstmechanismdevelopedforuseontheDigitalNetworkArchitecture(DNA).
* Theideaistoevenlysplittheresponsibilityforcongestioncontrolbetweenthe routers and the end nodes.
* Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur.
* Thisnotificationisimplemented bysettingabinarycongestion bitinthepackets that flow through the router; hence the name DECbit.
* The destination host thencopies thiscongestion bit intothe ACK itsends backto the source.
* TheSourcechecks*howmany*ACKhasDECbitsetforpreviouswindowpackets.
* Iflessthan50%ofACKhaveDECbitset,thensource*increases*itscongestion window by 1 packet
* Otherwise,*decreases*thecongestionwindowby87.5%.
* Finally,thesourceadjustsitssendingratesoastoavoidcongestion.
* *Increaseby1,decreaseby0.875*rulewasbasedonAIMDforstabilization.
* Asinglecongestionbitisaddedtothepacketheader.
* Usingaqueuelengthof1asthetriggerforsettingthecongestionbit.
* Arouter sets this bit ina packet if its average queue length is greater than or equal to 1 at the time the packet arrives.

ComputingaveragequeuelengthatarouterusingDECbit

****

* Averagequeuelengthismeasuredoveratimeintervalthatincludesthe

***lastbusy*+*lastidlecycle*+*currentbusy*cycle.**

* Itcalculatestheaveragequeuelengthby*dividing*thecurveareawithtimeinterval.

#### Red-RandomEarlyDetection

* The secondmechanismofcongestionavoidanceis calledasR*andomEarly Detection (RED).*
* Each router is programmed to monitor its own queue length, and when it detects that there is congestion, itnotifies the source to adjust its congestion window.
* REDdiffersfromtheDECbitschemebytwoways:

1. In DECbit, explicit notification about congestion is sent to source, whereas RED implicitly notifies the source by dropping a few packets.
2. DECbit may lead to tail drop policy, whereas RED drops packet based ondrop probability in a random manner. Drop each arriving packet with some ***drop probability*** whenever the queue length exceeds some *drop level.* This idea is *called* ***early random drop****.*

ComputationofaveragequeuelengthusingRED

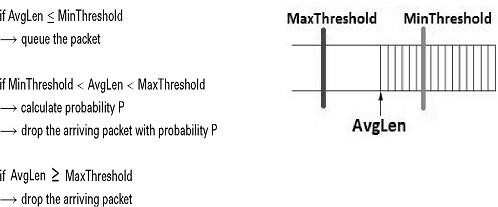
* AvgLen=(1−Weight)×AvgLen+Weight×SampleLen

where 0<Weight<1 and

SampleLen–isthelengthofthequeuewhena

samplemeasurementismade.

* Thequeuelengthismeasuredeverytimeanewpacketarrivesatthegateway.
* REDhastwoqueuelengththresholdsthattriggercertainactivity: ***MinThresholdand MaxThreshold***
* WhenapacketarrivesatagatewayitcomparesAvglenwiththesetwovalues according to the following rules.



**6. STREAMCONTROLTRANSMISSIONPROTOCOL(SCTP)**

* StreamControlTransmissionProtocol(SCTP)isareliable,message-oriented transport layer protocol.
* SCTPhasmixedfeaturesofTCPand UDP.
* SCTP maintainsthemessageboundariesanddetectsthelostdata,duplicatedataas well as out-of-order data.
* SCTPprovidestheCongestioncontrolaswellasFlowcontrol.
* SCTPisespeciallydesignedforinternetapplicationsaswellasmultimedia communication.

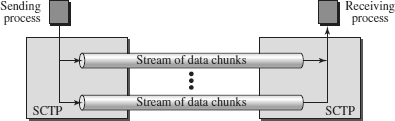
### SCTPSERVICES

Process-to-ProcessCommunication

* SCTPprovidesprocess-to-processcommunication.

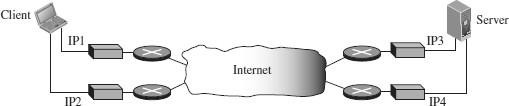
MultipleStreams

* SCTP allows multistream service in each connection, which is called ***association*** in SCTP terminology.
* Ifoneofthestreamsisblocked,theotherstreamscanstilldelivertheirdata.



Multihoming

* AnSCTPassociationsupportsmultihomingservice**.**
* The sending and receiving host can define multiple IP addresses in each end for anassociation.
* In this fault-tolerant approach, when one path fails, another interface can be used for data delivery without interruption.



Full-DuplexCommunication

* SCTP offers full-duplex service, where data can flow in both directions at the same time. Each SCTPthenhasasendingandreceivingbufferandpacketsaresentinboth directions.

Connection-OrientedService

* SCTPisaconnection-orientedprotocol.
* In SCTP,aconnectioniscalledan*association*.
* Ifaclientwantstosendandreceivemessagefromserver,thestepsare:

**Step1:**Thetwo**SCTPs**establishtheconnectionwitheachother.

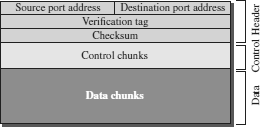
**Step2:**Oncetheconnectionisestablished,thedatagetsexchangedinboththe directions.

**Step3:**Finally,theassociationisterminated.

ReliableService

* SCTPisareliabletransportprotocol.
* Itusesanacknowledgment mechanismtocheckthesafeandsoundarrivalofdata.

### SCTPPACKETFORMAT

****

AnSCTPpackethasamandatorygeneralheaderandasetofblockscalledchunks.

#### GeneralHeader

* The*generalheader*(packetheader)definestheendpointsofeachassociationto which the packet belongs
* Itguaranteesthatthepacketbelongstoaparticularassociation
* Italsopreservestheintegrityofthecontentsofthepacketincludingtheheaderitself.
* Therearefourfieldsinthegeneralheader.

Sourceport

Thisfieldidentifiesthesendingport.

Destinationport

This field identifies the receiving port that hosts use to route the packet to the appropriate endpoint/application.

Verificationtag

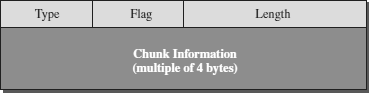
A32-[bit](https://en.wikipedia.org/wiki/Bit)randomvaluecreated duringinitializationtodistinguishstale packets from a previous connection.

Checksum

The next field is a checksum. The size of the checksum is 32 bits. SCTP uses CRC-32 Checksum.

#### Chunks

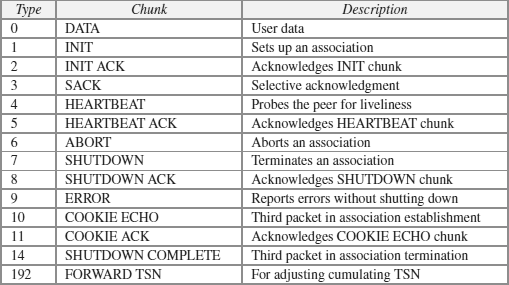
* Controlinformationoruserdataarecarriedinchunks.
* Chunkshaveacommonlayout.
* The first three fields are common to all chunks; the information field depends on the type of chunk.



* Thetypefieldcandefineupto256typesofchunks.Onlyafewhavebeendefinedso far; the rest are reserved for future use.
* Theflagfielddefinesspecialflagsthataparticularchunkmayneed.
* The length field defines the total size of the chunk, in bytes, including the type, flag, and length fields.

##### TypesofChunks

* An SCTP association may send many packets, a packet may contain several chunks, and chunks may belong to different streams.
* SCTPdefinestwotypesofchunks-ControlchunksandDatachunks.
* Acontrolchunkcontrolsandmaintainstheassociation.
* Adatachunkcarriesuserdata.

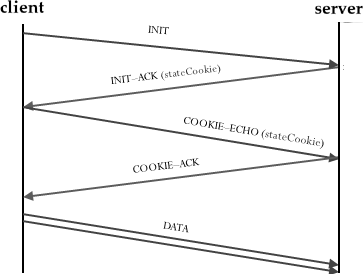


### SCTPASSOCIATION

* SCTPisaconnection-orientedprotocol.
* AconnectioninSCTPiscalledan*association*toemphasizemultihoming.
* SCTPAssociationsconsistsofthreephases:
* AssociationEstablishment
* DataTransfer
* AssociationTermination

#### AssociationEstablishment

* AssociationestablishmentinSCTPrequiresafour-wayhandshake.
* Inthisprocedure,aclientprocesswantstoestablishanassociationwithaserver processusing SCTP as the transport-layer protocol.
* TheSCTPserverneedstobepreparedtoreceiveanyassociation(passiveopen).
* Associationestablishment,however,isinitiatedbytheclient(activeopen).



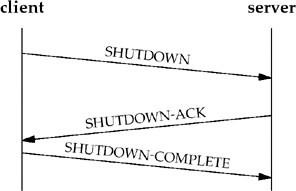
* Theclientsendsthefirstpacket,whichcontainsanINITchunk.
* The server sends the second packet, which contains an INIT ACK chunk. The INIT ACK also sends a cookie that defines the state of the server at this moment.
* The client sends the third packet, which includes a COOKIE ECHO chunk. This is a very simple chunk that echoes, without change, the cookie sent by the server. SCTP allows the inclusion of data chunks in this packet.
* The server sends the fourth packet, which includes the COOKIE ACK chunk that acknowledges the receipt of the COOKIE ECHO chunk. SCTP allows the inclusion of data chunks with this packet.

#### DataTransfer

* Thewholepurposeofanassociationistotransferdatabetweentwoends.
* Aftertheassociationisestablished,bidirectionaldatatransfercantakeplace.
* Theclientandtheservercanbothsenddata.
* SCTPsupportspiggybacking.
* TypesofSCTPdataTransfer:
  1. MultihomingDataTransfer
     + Datatransfer,bydefault,usestheprimaryaddressofthedestination.
     + Iftheprimaryisnotavailable,oneofthealternativeaddressesisused.
     + ThisiscalledMultihomingDataTransfer.
  2. MultistreamDelivery
     + SCTP can support multiple streams, which means that the sender process can define different streams and a message can belong to one of these streams.
     + Each stream is assigned a stream identifier (SI) which uniquely definesthat stream.
     + SCTPsupportstwotypesofdatadeliveryineachstream: *ordered*(default) and *unordered.*

#### AssociationTermination

* In SCTP,either of the two parties involved in exchanging data (client or server) can close the connection.
* SCTP does not allow a “half closed” association. If one end closes the association,the other end must stop sending new data.
* If any data are left over in the queue of the recipient of the termination request, they are sent and the association is closed.
* Associationterminationusesthreepackets.

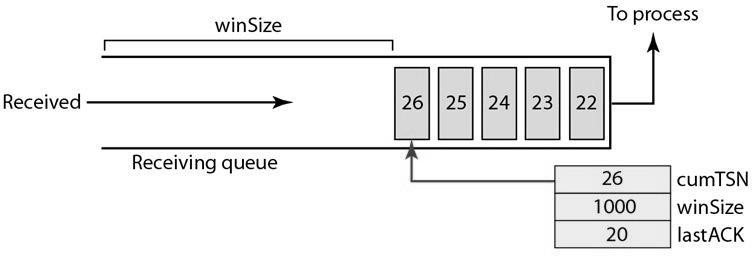


### SCTPFLOWCONTROL

* FlowcontrolinSCTPissimilartothatin TCP.
* CurrentSCTPimplementationsuseabyte-orientedwindowforflowcontrol.

#### ReceiverSite

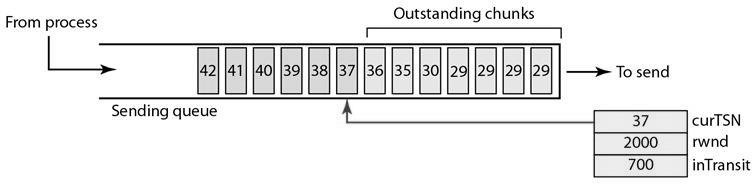
* Thereceiverhasonebuffer(queue)andthreevariables.
* Thequeueholdsthereceiveddatachunksthathavenotyetbeenreadbytheprocess.
* ThefirstvariableholdsthelastTSNreceived,cumTSN.
* Thesecondvariableholdstheavailablebuffersize;winsize.
* Thethirdvariableholdsthelastaccumulativeacknowledgment,lastACK.
* Thefollowingfigureshowsthequeueandvariablesatthereceiversite.



* When the site receives a data chunk, it stores it at the end of the buffer (queue) and subtracts the size of the chunk from winSize.
* TheTSNnumberofthechunkisstoredinthecumTSNvariable.
* Whentheprocessreadsachunk,itremovesitfromthequeueandaddsthesizeofthe removed chunk to winSize (recycling).
* WhenthereceiverdecidestosendaSACK, itchecksthe valueoflastAck;ifitisless than cumTSN, it sends a SACK with a cumulative TSN number equal to the cumTSN.
* ItalsoincludesthevalueofwinSizeastheadvertisedwindowsize.

#### SenderSite

* Thesenderhasonebuffer(queue)andthreevariables:curTSN,rwnd,andinTransit.
* We assume each chunk is 100 bytes long. The buffer holds the chunks produced by the process that either have been sent or are ready to be sent.
* Thefirstvariable,curTSN,referstothenextchunktobesent.
* AllchunksinthequeuewithaTSNlessthanthisvaluehavebeensent,butnot acknowledged; they are outstanding.
* Thesecondvariable,rwnd,holdsthelastvalueadvertisedbythereceiver(inbytes).
* The third variable, inTransit, holds the number of bytes in transit, bytes sent but not yet acknowledged.
* Thefollowingfigureshowsthequeueandvariablesatthesendersite.



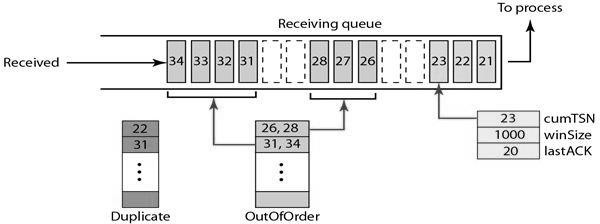
* Achunkpointed to by curTSN can be sent if the size of the data is less than or equal to the quantity rwnd - inTransit.
* After sendingthe chunk, the value of curTSN is incremented by 1 and now points to the next chunk to be sent.
* ThevalueofinTransitisincrementedbythesizeofthedatainthetransmittedchunk.
* When a SACK is received, the chunks with a TSN less than or equal to the cumulativeTSNinthe SACKareremovedfromthequeueanddiscarded. Thesender does not have to worry about them anymore.
* ThevalueofinTransitisreducedbythetotalsizeofthediscardedchunks.
* ThevalueofrwndisupdatedwiththevalueoftheadvertisedwindowintheSACK.

### SCTPERRORCONTROL

* SCTPisareliabletransportlayerprotocol.
* ItusesaSACKchunktoreportthestateofthereceiverbuffertothesender.
* Each implementation uses a different set of entities and timers for the receiver andsender sites.

#### ReceiverSite

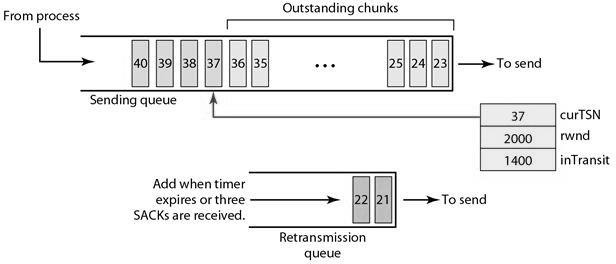
* Thereceiverstoresallchunksthathavearrivedinitsqueueincludingtheout-of- order ones. However, it leaves spaces for any missing chunks.
* Itdiscardsduplicatemessages,butkeepstrackofthemforreportstothesender.
* The following figure shows a typical design for the receiver site and the state of the receiving queue at a particular point in time.



* Theavailablewindowsizeis1000bytes.
* Thelastacknowledgmentsentwasfordatachunk20.
* Chunks21to23havebeenreceivedinorder.
* Thefirstout-of-orderblockcontainschunks26to 28.
* Thesecondout-of-orderblockcontainschunks31to34.
* AvariableholdsthevalueofcumTSN.
* An array of variables keeps track of the beginning and the end of each block that isout of order.
* Anarrayofvariablesholdstheduplicatechunksreceived.
* Thereisnoneedforstoringduplicatechunksinthequeueandtheywillbediscarded.

#### SenderSite

* Atthesendersite,itneedstwobuffers(queues):asendingqueueanda retransmission queue.
* Threevariableswereused-rwnd,inTransit,andcurTSNasdescribedintheprevious section.
* Thefollowingfigureshowsatypicaldesign.



* Thesendingqueueholdschunks23to 40.
* The chunks 23 to 36 have already been sent, but not acknowledged; they are outstanding chunks.
* ThecurTSNpointstothenextchunktobesent(37).
* Weassumethateachchunkis100bytes,whichmeansthat1400bytesofdata (chunks 23 to 36) is in transit.
* Thesenderatthismomenthasaretransmissionqueue.
* Whenapacketissent, aretransmissiontimerstartsforthatpacket(alldatachunksin that packet).
* Someimplementationsuseonesingletimerfortheentireassociation,butother implementations use one timer for each packet.

### SCTPCONGESTIONCONTROL

* SCTPisatransport-layerprotocolwithpacketssubjecttocongestioninthenetwork.
* TheSCTPdesignershaveusedthesamestrategiesforcongestioncontrolasthose used in TCP.

**NOTE:REFERTCPCONGESTIONCONTROL**

**UNIT5:APPLICATIONLAYER**

**WWWandHTTP–FTP– Email–Telnet–SSH–DNS– SNMP**

## 1.INTRODUCTION

* Theapplicationlayeristhehighestlayerintheprotocolsuite.
* Theapplicationlayerprovidesservicestotheuser.
* Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages.
* TheapplicationlayeristheonlylayerthatprovidesservicestotheInternetuser
* Theapplicationlayerexchangemessageswith theirpeersonothermachines
* Applications need their own protocols. These applications are part of network protocol.
* TypesofApplicationProtocols:

StandardandNonstandardProtocols

**StandardApplication-LayerProtocols**

* + Thereareseveralapplication-layerprotocolsthathavebeenstandardized and documented by the Internet authority.
  + Each standard protocol is a pair of computer programs that interact with the user and the transport layer to provide a specific service to the user.
  + Twoverywidely-usedstandardizedapplicationprotocols:

**SMTP** : Simple Mail Transfer Protocol is used to exchange electronicmail.

**HTTP**:HyperTextTransportProtocolisusedtocommunicate between Web browsers and Web servers.

**NonstandardApplication-LayerProtocols**

* + A programmer can create a nonstandard application-layer program if they can write two programs that provide service to the user by interacting with the transport layer.

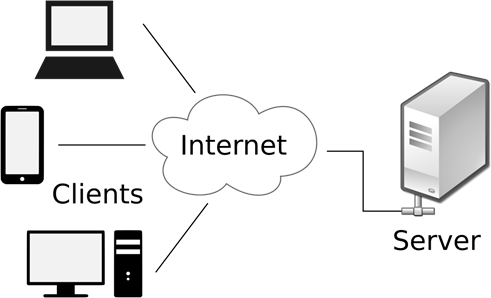
### APPLICATION-LAYERPARADIGMS

TwoparadigmshavebeendevelopedforApplicationLayer

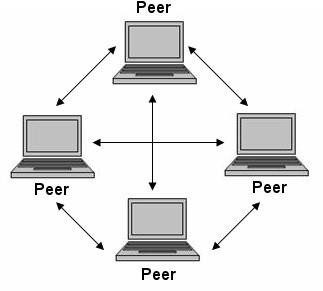
1. TraditionalParadigm:Client-Server
2. **NewParadigm: Peer-to-Peer**

**Client-ServerParadigm**

* + The**traditionalparadigm**iscalledtheclient-serverparadigm.
  + ItwasthemostpopularParadigm.
  + In this paradigm, the service provider is an application program, called the server process; it runs continuously, waiting for another application program, called the client process, to make a connection throughthe Internet and ask for service.
  + The server process must be runningall the time; the client process is started when the client needs to receive service.
  + There are normally some server processes that can provide a specific typeof service, but there are many clients that request service from any of these server processes.



**Peer-to-Peer(P2P)Paradigm**

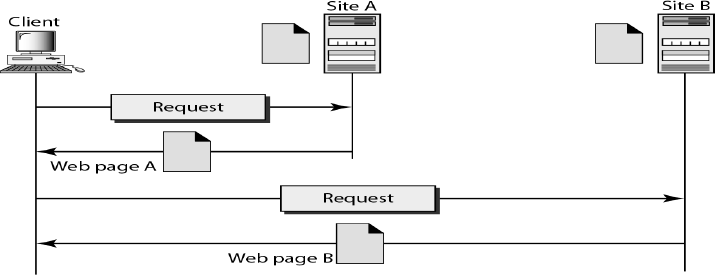
* A**newparadigm**,calledthepeer-to-peerparadigmhasemergedtorespondto the needs of some newapplications.
* Inthisparadigm,thereisnoneedforaserverprocesstoberunningallthetime and waiting for the client processes to connect.
* Theresponsibilityissharedbetweenpeers.
* AcomputerconnectedtotheInternetcanprovideserviceatonetimeand receive service at another time.
* Acomputercanevenprovideandreceiveservicesatthesametime.

**MixedParadigm**

* An applicationmaychoose touseamixtureofthetwoparadigmsby combining the advantages of both.
* For example, a light-load client-server communication can be used to find the address of the peer that can offer a service.
* When the address of the peer is found, the actual service can be received from the peer by using the peer-to-peer paradigm.

## 2.WWW(WORLDWIDEWEB)

* WWWisadistributedclient/serverservice,in whichaclient(Browserssuchas IE, Firefox, etc.) can access services at a server (Web server such as IIS, Apache).
* Theserviceprovidedisdistributedovermanylocationscalledsites.
* WWW was constructed originally by a small group of people led by Tim Berners Lee at CERN, in 1989 and in 1991 this was released to the world.
* A new protocol for the Internet and a system of document access to use it was proposed and named as [WWW.](http://www/)



* ThissystemallowsdocumentsearchandretrievalfromanypartoftheInternet.
* Thedocumentswerehaving*Hypertext*asthecontent
* The units of information on the web can be referred to as pages, documents or resources.
* A document can contain text, images, sound and video, together called Hypermedia.
* Web is a vast collection of data, information, software and protocols , spread across the world in web servers, which are accessed by client machines by browsers through the Internet.

### COMPONENTSOFTHEWEB

**StructuralComponents**

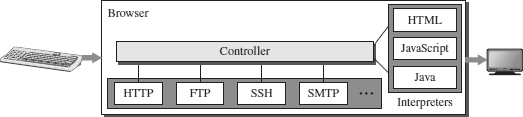
* 1. WebClients/Browsers
  2. WebServers
  3. WebCaches
  4. Internet

**SemanticComponents**

1. HyperTextTransferProtocol(HTTP)
2. HyperTextMarkupLanguage(HTML)
3. eXtensibleMarkupLanguage(XML)
4. UniformResourceIdentifier(URI)
   * Clients use browser application to send URL’s via HTTP to servers requesting a Web page.
   * Web pages constructed usingHTML/XMLand consist of text, graphics, sounds plus embedded files
   * Servers(orcaches)respondwithrequestedWebpage.
   * Client’sbrowserrendersWebpagereturnedbyserver
   * WebPageiswrittenusingHyperTextMarkupLanguage(HTML)
   * Displaystext,graphicsandsoundinbrowser
   * Theentiresystemrunsoverstandardnetworkingprotocols(TCP/IP,DNS)

WEBCLIENTS(BROWSERS)

* + Abrowserisasoftwareontheclientonthewebwhichinitiatesthe communication with the server.
  + Eachbrowserusuallyconsistsofthreeparts:acontroller,clientprotocols,and interpreters.
  + The controller receives input from the keyboard or the mouse and uses the clientprogramstoaccessthedocument.Afterthedocumenthasbeenaccessed, the controller uses one of the interpreters to display the document on the screen.
  + Examples areInternet Explorer,MozillaFireFox, NetscapeNavigator,Safari etc.

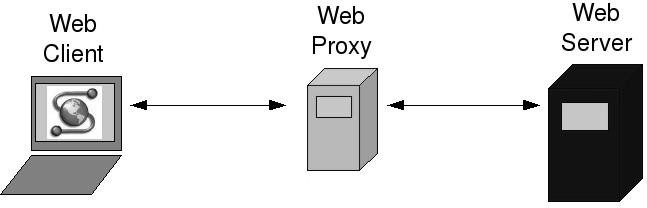


WEBSERVERS

* + All the communication between the web client and a webserver use the standard protocol called as HTTP.
  + Webserverinformsitsoperatingsystemtoacceptincomingnetwork connections using a specific port on the machine.
  + Theserveralsorunsasabackgroundprocess.
  + A client (browser) opens a connection to the server, sends a request, receivesinformation from server and closes the connection.
  + Web server monitors a communications port on its host machine, accepts thehttp commands through it and performs specified operations.
  + HTTPcommandsincludeaURLspecifyingthehostmachine.
  + The URL received is translated into either a filename or a program name, accordingly the requested file or the output of the program execution is sent back to the browser.

PROXYSERVER

* AProxyserverisacomputerthatkeepscopiesofresponsestorecentrequests.
* Thewebclientsendsarequesttotheproxyserver.
* Theproxyserverchecksitscache.
* If the response is not stored in the cache, the proxy server sends the request to the corresponding server.



* Incoming responses are sent to the proxy server and stored for future requests from other clients.
* The proxy server reduces the load on the original server, decreases traffic, and improves latency.
* However, to use the proxy server, the client must be configured to access theproxy instead of the target server.
* Theproxyserveractsasbothserverandclient.
* When it receives a request froma client for which it has a response, it acts as a server and sends the response to the client.
* When it receives a request from a client for which it does not have a response, it first acts as a client and sends a request to the target server.
* Whentheresponsehasbeenreceived,itactsagainasaserverandsendsthe response to the client.

### URL-UNIFORMRESOURCELOCATOR

* + UniformResourceLocator(URL),uniquelyidentifyresourcesontheInternet
  + URLprovidesinformationaboutitslocationontheWeb
  + When a user enters URL, browser forms a *request* message and sends it to the server.
  + WebserverretrievestherequestedURLandsendsbacka*response*message.
  + WebbrowserrenderstheresponseinHTMLorappropriateformat.
  + Format:http://www.*domain\_name*/*filename*
  + Example:<http://www.cs.hello.org/index.html>



* + TheURLdefinesfourparts-Method,Hostcomputer,Port,andPath.
* **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
* **Host:** The host is the computer where the information is stored, and the computeris givenanaliasname. Webpagesaremainlystoredinthecomputers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
* **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
* **Path:** Path is the pathname of thefile wherethe information is stored. Thepath itself contain slashes that separate the directories from the subdirectories and files.

**URLPaths**

* + The path of the document for a http protocol is same as that for a document or file or a directory in a client.
  + InUnixthepathcomponentsareseparatedbyforwardslashes(/)andin windows backward slashes (\).
  + ButanURLneednotincludeallthedirectoriesinthepath.
  + Apathwhichincludesallthedirectoriesisa***completepath***,elseitisa

partialpath.

**URI-UniformResourceIdentifiers**

* + URIisastringthatidentifiesresourcessuchasdocument,image,service,etc.
  + Itisoftheform*scheme*:*scheme*-*specific*
  + Scheme*identifies*aresourcetype,suchasmailtoformailaddress,filefor file name, etc. and scheme-specific is a *resource* identifier.
  + Exampleismailto:[abc123@gmail.com](mailto:abc123@gmail.com)
  + URIidentifiesaresource,whereasURLisusedtolocatearesource.

### WEBDOCUMENTS

ThedocumentsintheWWWcanbegroupedintothreebroadcategories: Static, DynamicandActive.

**StaticDocuments**

* Static documents are fixed-content documents that are created and stored in aserver.
* Theclientcangetacopyofthedocumentonly.
* In other words, the contents of the file are determined when the file is created, not when it is used.
* Ofcourse,thecontentsintheservercanbechanged,buttheusercannotchange them.
* Whenaclientaccessesthedocument,acopyofthedocumentissent.
* Theusercanthenuseabrowsertoseethedocument.
* Staticdocumentsarepreparedusingoneofseverallanguages:
  1. HyperTextMarkupLanguage(HTML)
  2. ExtensibleMarkupLanguage(XML)
  3. ExtensibleStyleLanguage(XSL)
  4. ExtensibleHypertextMarkupLanguage(XHTML).

**DynamicDocuments**

* A dynamic document is created by a web server whenever a browser requests the document.
* When a request arrives, the web server runs an application program or a script that creates the dynamic document.
* Theserverreturnstheresultoftheprogramorscriptasaresponsetothe browser that requested the document.
* Becauseafreshdocumentiscreatedforeachrequest,thecontentsofadynamic document may vary from one request to another.
* A very simple example of a dynamic document is the retrieval of the time and date from a server.
* Timeanddatearekindsofinformationthataredynamicinthattheychange from moment to moment.
* Dynamicdocumentscanberetrievedusingoneofseveralscriptinglanguages:
  1. CommonGatewayInterface(CGI)
  2. JavaServerPages(JSP)
  3. ActiveServerPages(ASP)
  4. ColdFusion

**ActiveDocuments**

* Formanyapplications, weneedaprogramorascripttoberunattheclientsite. These are called active documents**.**
* For example, suppose we want to run a programthat creates animated graphics on the screen or a program that interacts with the user.
* The programdefinitely needs to be run atthe client site where the animation or interaction takes place.
* Whenabrowserrequestsanactivedocument,theserversendsacopyofthe document or a script.
* Thedocumentisthenrunattheclient(browser)site.
* Activedocumentscanbecreatedusingoneofseverallanguages:
  1. Java Applet – A program written in Java on the server. It is compiled andreadytoberun.Thedocumentisinbytecodeformat.
  2. JavaScript-Downloadandrunthescriptattheclientsite.

## 3. HTTP(HYPERTEXTTRANSFERPROTOCOL)

* TheHyperTextTransferProtocol(HTTP)isusedtodefinehowtheclient- server programs can be written to retrieve web pages from the Web.
* ItisaprotocolusedtoaccessthedataontheWorldWideWeb(WWW).
* TheHTTPprotocolcanbeused totransferthedatainthe form ofplaintext, hypertext, audio, video, and so on.
* HTTPisa*stateless*request/responseprotocolthatgovernsclient/server communication.
* AnHTTPclientsendsarequest;anHTTPserverreturnsaresponse.
* Theserverusestheportnumber80;theclientusesatemporaryportnumber.
* HTTPusestheservicesofTCP,aconnection-orientedandreliableprotocol.
* HTTPisatext-orientedprotocol.Itcontains*embedded*URLknownaslinks.
* When hypertext is clicked, browser opens anew connection, retrieves file from the server and displays the file.
* EachHTTPmessagehasthegeneral form

START\_LINE <CRLF> MESSAGE\_HEADER<CRLF>

<CRLF>MESSAGE\_BODY<CRLF>

where<CRLF>standsforcarriage-return-line-feed.

**FeaturesofHTTP**

* **Connectionlessprotocol:**

HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

* **Mediaindependent:**

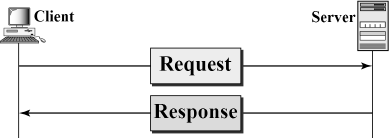
HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.

* **Stateless:**

HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

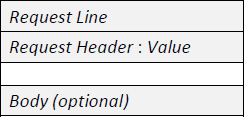
### HTTPREQUESTANDRESPONSEMESSAGES

* TheHTTPprotocoldefinestheformatoftherequestandresponsemessages.



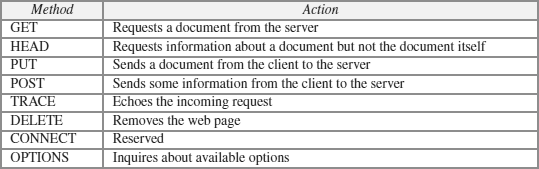
* **RequestMessage:**Therequestmessageissentbytheclientthatconsistsofa request line, headers, and sometimes a body.
* **Response Message:** The response message is sent by the server to the client thatconsistsofastatusline,headers,andsometimesabody.

HTTPREQUESTMESSAGE

****

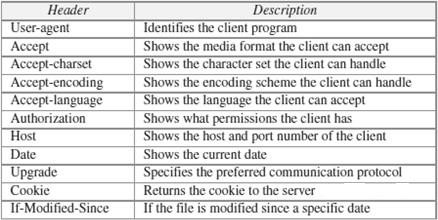
* Thefirstlineinarequestmessageiscalleda*requestline*.
* Aftertherequestline,wecanhavezeroormore*requestheader*lines.
* The *body* isan optionalone. It contains the comment to be sent orthe fileto be published on the website when the method is PUT or POST.

***RequestLine***

* Therearethreefieldsinthisrequestline-M*ethod,URL*andV*ersion*.
* TheMethodfielddefinestherequesttypes.
* TheURLfielddefinestheaddressandnameofthecorrespondingwebpage.
* TheVersionfieldgivestheversionoftheprotocol;themostcurrentversionof HTTP is 1.1.
* SomeoftheMethodtypesare

***RequestHeader***

* Eachrequestheaderlinesendsadditionalinformationfromtheclienttothe server.
* Eachheaderlinehasaheadername,acolon,aspace,andaheader value.
* Thevaluefielddefinesthevaluesassociatedwitheachheadername.
* Headersdefinedforrequestmessageinclude



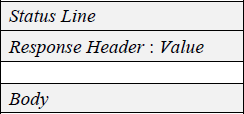
***Body***

* The*body*canbepresentinarequestmessage. Itisoptional.
* Usually,itcontainsthecommenttobesentorthefiletobepublishedonthe website when the method is PUT or POST.

***ConditionalRequest***

* Aclientcanaddaconditioninitsrequest.
* In this case, the server will send the requested web page if the condition is met or inform the client otherwise.
* One of the most common conditions imposed by the client is the time and date the web page is modified.
* Theclientcansendtheheaderline*If-Modified-Since*withtherequesttotellthe server that it needs the page only if it is modified after a certain point in time.

HTTPRESPONSEMESSAGE

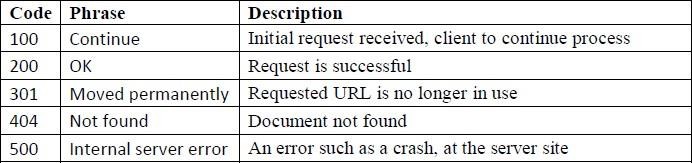
****

* Thefirstlineinarequestmessageiscalledastatus*line*.
* Aftertherequestline,wecanhavezeroormore*responseheader*lines.
* The *body* is anoptional one. Thebodyis present unless theresponse is anerror message

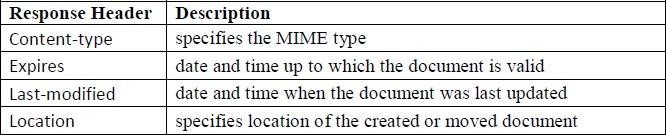
***StatusLine***

* TheStatuslinecontainsthreefields -*HTTPversion,Statuscode,Status phrase*
* ThefirstfielddefinestheversionofHTTPprotocol,currently 1.1.
* Thestatuscodefielddefinesthestatusoftherequest.ItclassifiestheHTTP result. It consists of three digits.

1*xx*–Informational, 2*xx*– Success, 3*xx*–Redirection, 4*xx*–Client error, 5*xx*–Server error

* TheStatusphrasefieldgivesbriefdescriptionaboutstatuscodeintextform.
* SomeoftheStatuscodesare

***ResponseHeader***

* Eachheaderprovidesadditionalinformationtotheclient.
* Eachheaderlinehasaheadername,acolon,aspace,andaheader value.
* Someoftheresponseheadersare:

***Body***

* Thebodycontainsthedocumenttobesentfromtheservertotheclient.
* Thebodyispresentunlesstheresponseisanerrormessage.

### HTTPCONNECTIONS

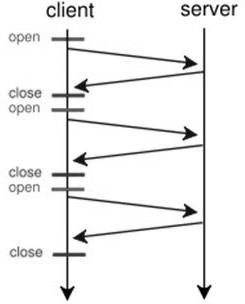
* HTTP Clients and Servers exchange multiple messages over the same TCP connection.
* If some of the objects are located on the same server, we have two choices: to retrieve each object using a new TCP connection or to make a TCP connection and retrieve them all.
* Thefirstmethodisreferredtoasa*non-persistentconnection,*thesecondasa

*persistentconnection*.

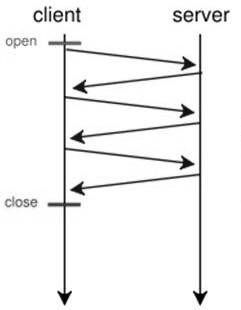
* HTTP1.0uses*non-persistent*connectionsandHTTP1.1uses*persistent*

connections.

NON-PERSISTENTCONNECTIONS

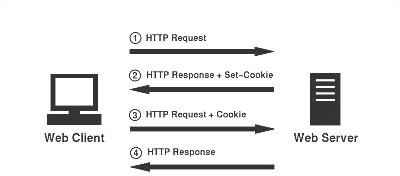
* In a non-persistent connection, one TCP connection is made for each request/response.
* Onlyoneobjectcan besentover asingle TCP connection
* The client opens a TCP connection and sends a request.
* The server sends the response and closes the connection.
* The client reads the data until it encounters an end-of-file marker.
* Itthenclosesthe connection.

PERSISTENTCONNECTIONS

* HTTPversion1.1specifiesapersistentconnection by default.
* Multiple objects can be sent over a single TCP connection.
* In a persistent connection, the server leaves the connection open for more requests after sending a response.
* The server can close the connection at the request of a client or if a time-out has been reached.
* Time and resources are saved using persistent connections. Only one set of buffers and variables needs to be set for the connection at each site.
* The round trip time for connectionestablishment and connection termination is saved.

### HTTPCOOKIES

* + An**HTTP cookie** (also called **web cookie**, **Internet cookie**, **browser cookie**, or simply **cookie**) is a small piece of data sentfroma website and stored on the user's computer by the user's web browser while the user is browsing.
  + HTTPisstateless,CookiesareusedtoaddState.
  + Cookiesweredesignedtobeareliablemechanismforwebsitesto remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past).
  + They can also beused toremember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers.



**ComponentsofCookie**

Acookieconsistsofthefollowingcomponents:

1. Name
2. Value
3. Zeroormore attributes(name/valuepairs). Attributes storeinformationsuch as the cookie's expiration, domain, and flags

#### CreatingandStoringCookies

The creation and storing of cookies depend on the implementation; however, the principle is the same.

* 1. When a server receives a request from a client, it stores information about the client in a file or a string. The information may include the domain name of the client, the contents of the cookie (information the server has gathered about the client such as name, registration number, and so on), a timestamp, and other information depending on the implementation.
  2. Theserverincludesthecookieintheresponsethatitsendstotheclient.
  3. When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the server domain name.

#### UsingCookies

* Whenaclientsendsarequesttoaserver,thebrowserlooksinthecookie directory to see if it can find a cookie sent by that server.
* Iffound,thecookieisincludedintherequest.
* When the serverreceives the request,it knowsthatthis is an old client, not a new one.
* Thecontentsofthecookieareneverreadbythebrowserordisclosedtothe user. It is a cookie *made* by the server and *eaten* by the server.

**TypesofCookies**

1. **Authenticationcookies**

These are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in.

1. **Trackingcookies**

Thesearecommonlyusedaswaystocompileindividualsbrowsinghistories.

1. Sessioncookie

Asession cookie exists only in temporary memory while the user navigates the website. Web browsers normally delete session cookies when the user closes the browser.

1. Persistentcookie

Insteadofexpiringwhenthewebbrowserisclosedassessioncookiesdo,a persistent cookie expires at a specific date or after a specific length of time. This means that, for the cookie's entire lifespan , its information will be transmittedtotheservereverytimetheuser visitsthewebsitethatitbelongsto, or every time the user views a resource belonging to that website from another website.

### HTTPCACHING

* + HTTP Caching enables the client to retrieve document *faster* and reduces load on the server.
  + HTTPCachingisimplementedatProxyserver,ISProuterandBrowser.
  + Server sets *expiration* date (Expires header) for each page, beyond which it is not cached.
  + HTTPCachedocumentisreturnedtoclientonlyifitisan*updated*copyby checking against If-Modified-Since header.
  + Ifcachedocumentis *out-of-date*,thenrequestis forwardedtotheserverand response is cached along the way.
  + Awebpagewillnotbecachedif*no-cache*directiveisspecified.

### HTTPSECURITY

* + HTTPdoesnotprovidesecurity.
  + HoweverHTTPcanberunovertheSecureSocketLayer(SSL).
  + Inthiscase,HTTPisreferredtoasHTTPS.
  + HTTPSprovidesconfidentiality,clientandserverauthentication,anddata integrity.

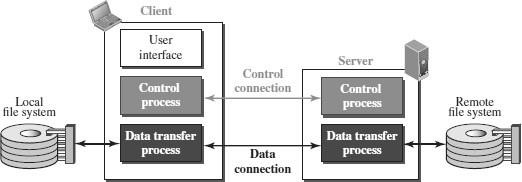
**4. FTP(FILETRANSFERPROTOCOL)**

* + - FTPstandsforFiletransferprotocol.
    - FTPisastandardinternetprotocolprovidedbyTCP/IPusedfor transmitting the files from one host to another.
    - It is mainly used for transferringthe web page files fromtheir creator to the computer that acts as a server for other computers on the internet.
    - Itisalsousedfordownloadingthefilestocomputerfromotherservers.
    - AlthoughwecantransferfilesusingHTTP, FTPisabetterchoiceto transfer large files or to transfer files using different formats.

### FTPOBJECTIVES

* + - Itprovidesthesharingoffiles.
    - Itisusedtoencouragetheuseofremotecomputers.
    - Ittransfersthedatamorereliablyandefficiently.

### FTPMECHANISM

****

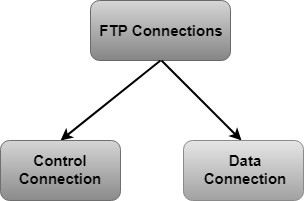
* + TheabovefigureshowsthebasicmodeloftheFTP.
  + TheFTPclienthasthreecomponents:
* userinterface,controlprocess,anddatatransferprocess.
  + Theserverhastwocomponents:
* servercontrolprocessandserverdatatransfer process.

### FTP CONNECTIONS

* + TherearetwotypesofconnectionsinFTP-

ControlConnectionandDataConnection.

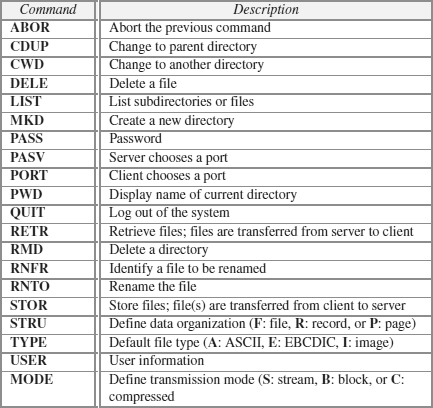
* + ThetwoconnectionsinFTPhavedifferentlifetimes.
  + ThecontrolconnectionremainsconnectedduringtheentireinteractiveFTP session.
  + Thedataconnectionisopenedandthenclosedforeachfiletransferactivity. When a user starts an FTP session, the control connection opens.
  + While the control connectionis open, the dataconnection can be openedand closed multiple times if several files are transferred.
  + FTPusestwowell-knownTCPports:
* Port21isusedforthecontrol connection
* Port20isusedforthedataconnection.



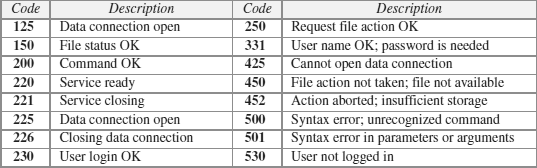
* + ControlConnection:
* Thecontrolconnectionusesverysimplerulesforcommunication.
* Through control connection, we can transfer a line of command or line of response at a time.
* Thecontrolconnectionismadebetweenthecontrolprocesses.
* The control connection remains connected during the entire interactive FTP session.
  + DataConnection:
* TheDataConnectionusesverycomplexrulesasdatatypesmayvary.
* Thedataconnectionismadebetweendatatransferprocesses.
* Thedataconnectionopenswhenacommandcomesfortransferringthe files and closes when the file is transferred.

### FTP COMMUNICATION

* + FTPCommunicationisachievedthroughcommandsandresponses.
  + FTPCommandsaresentfromtheclienttotheserver
  + FTPresponsesaresentfromtheservertotheclient.
  + FTP Commands are in the formof ASCIIuppercase, which may or may not be followed by an argument.
  + Someofthemostcommoncommandsare



* + EveryFTPcommandgeneratesatleastoneresponse.
  + Aresponsehastwoparts:athree-digitnumberfollowedbytext.
  + Thenumericpartdefinesthecode;thetextpartdefinesneededparameter.



### FTPFILE TYPE

* + FTPcantransferoneofthefollowingfiletypesacrossthedataconnection: ASCII file, EBCDIC file, or image file.

### FTPDATASTRUCTURE

* + FTP can transfer a file across the data connection using one of the following data structure : *file structure, record structure,* or *page structure*.
  + The file structure format is the default one and has no structure. It is a continuous stream of bytes.
  + In the record structure, the file is divided into *records*. This can be used only with text files.
  + In the page structure, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially.

### FTPTRANSMISSIONMODE

* + FTPcantransfera fileacross thedata connectionusing oneofthefollowing three transmission modes: *stream mode, block mode,* or *compressed mode*.
  + The stream mode is the default mode; data are delivered fromFTP to TCP as a continuous stream of bytes.
  + Intheblockmode,datacanbedeliveredfromFTPtoTCPinblocks.
  + In the compressedmode,data can be compressed and deliveredfrom FTP toTCP.

FTPFILETRANSFER

* + Filetransferoccursoverthedataconnectionunderthecontrolofthe commands sent over the control connection.
  + FiletransferinFTPmeansoneofthreethings:
* retrievingafile(servertoclient)
* storingafile(clienttoserver)
* directorylisting(servertoclient).

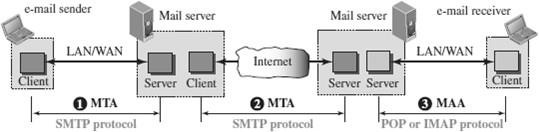
### FTP SECURITY

* + FTPrequiresapassword,thepasswordissentinplaintextwhichis unencrypted. This means it can be intercepted and used by an attacker.
  + Thedatatransferconnectionalsotransfersdatainplaintext,whichisinsecure.
  + To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer.
  + InthiscaseFTPiscalledSSL-FTP.

**5. EMAIL(SMTP,MIME,IMAP,POP)**

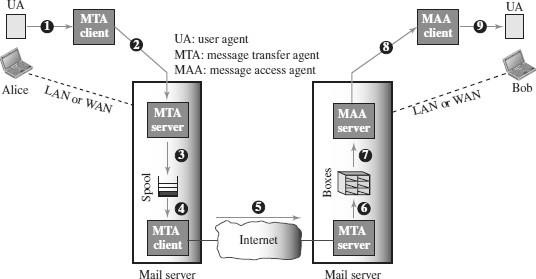
* + OneofthemostpopularInternetservicesiselectronicmail(E-mail).
  + Emailisoneoftheoldestnetworkapplications.
  + ThethreemaincomponentsofanEmailare

1. UserAgent(UA)
2. MesssageTransferAgent(MTA)–SMTP
3. MesssageAccessAgent(MAA)-IMAP,POP



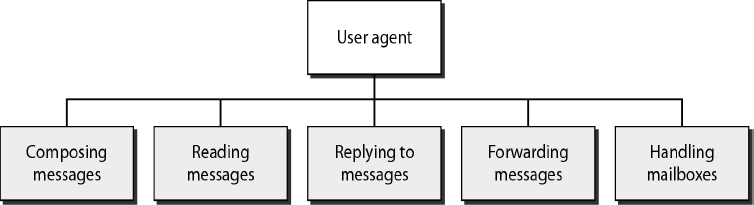
* + When the sender andthe receiver of ane-mail are on thesame system, we need only two User Agents and no Message Transfer Agent
  + When the sender and the receiver of an e-mail are on different system, we need two UA, two pairs of MTA (client and server), and two MAA (client and server).

WORKINGOFEMAIL

****

* + When Alice needs to send a message toBob, she runs a UA program to prepare the message and send it to her mail server.
  + The mail server at her site uses a queue (spool) to store messages waiting to be sent. The message, however, needs to be sent through the Internet from Alice’s site to Bob’s site using an MTA.
  + Heretwomessagetransferagentsareneeded:oneclientandoneserver.
  + Theserverneedstorunallthetimebecauseitdoesnotknowwhenaclientwill ask for a connection.
  + The client can be triggered by the systemwhen there is a message in the queue to be sent.
  + TheuseragentattheBobsiteallowsBobtoreadthereceivedmessage.
  + BoblaterusesanMAAclienttoretrievethemessagefromanMAAserver running on the second server.

USERAGENT(UA)

* + Thefirstcomponentofanelectronicmailsystemistheuseragent(UA).
  + It provides service to the user to make the process of sending and receiving amessage easier.
  + A user agent is a software package that composes, reads, replies to, and forwardsmessages.Italsohandleslocalmailboxesontheusercomputers.
  + Therearetwotypesofuseragents:**Command-drivenandGUI-based**.

Commanddriven

* Commanddrivenuseragentsbelongtotheearlydaysofelectronicmail.
* Acommand-drivenuseragentnormallyacceptsaonecharactercommandfrom the keyboard to perform its task.
* Someexamplesofcommanddrivenuseragentsare*mail,pine,*and*elm*.

GUI-based

* ModernuseragentsareGUI-based.
* Theyallowthe userto interact withthe softwarebyusing boththe keyboard and the mouse.
* They have graphical components such as icons, menu bars, and windows thatmake the services easy to access.
* SomeexamplesofGUI-baseduseragentsare*Eudora*and*Outlook***.**

MESSAGETRANSFERAGENT(MTA)

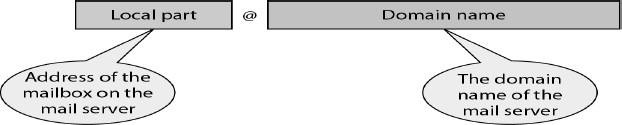
* + Theactualmailtransferisdonethroughmessagetransferagents(MTA).
  + Tosendmail,asystemmusthavetheclientMTA,andtoreceivemail,a system must have a server MTA.
  + Theformalprotocolthatdefines theMTA clientandserverin theInternetis called Simple Mail Transfer Protocol (SMTP).

MESSAGEACCESSAGENT(MAA)

* + MAAisasoftwarethatpullsmessagesoutofamailbox.
  + POP3andIMAP4areexamplesofMAA.

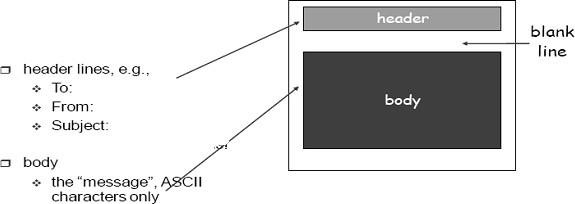
ADDRESSFORMATOFEMAIL

* + E-mailaddressis*userid*@*domain*where*domain*ishostnameofthe*mail server*.



MESSAGEFORMATOFEMAIL

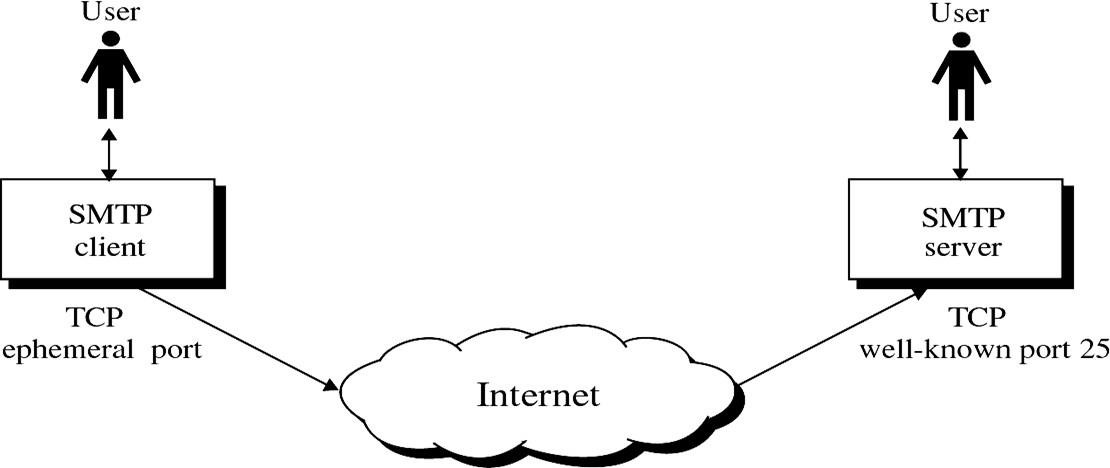
* + Emailmessageconsistsoftwopartsnamely*header*and*body*.
  + Eachheaderlinecontains*type*and*value*separatedbyacolon(:).
  + Someheadercontentsare:
* **From:**identifiersenderofthemessage.
* **To:** mailaddressoftherecipient(s).
* **Subject:**saysaboutpurposeofthemessage.
* **Date:**timestampofwhenthemessagewastransmitted.
  + Headerisseparatedfromthebodybya*blank*line.
  + Bodycontainsthe*actual*message.



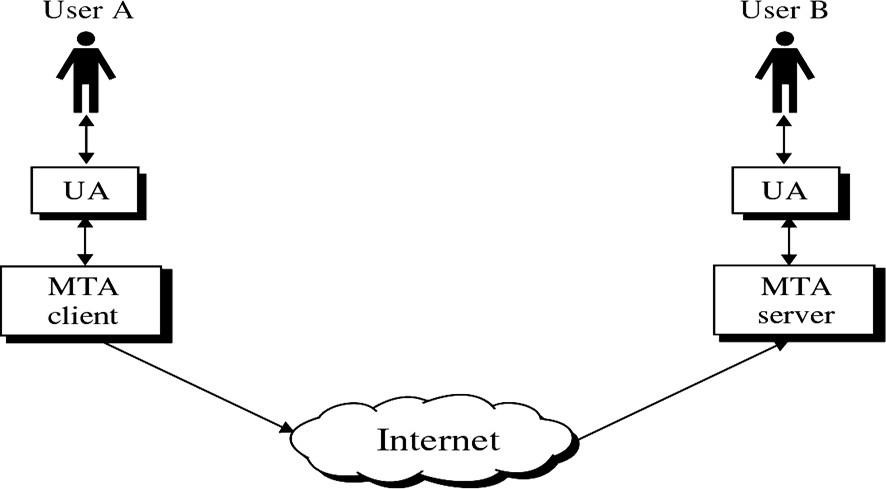
* + - Emailwasextendedin1993tocarrymanydifferenttypesofdata:audio, video, images, Word documents, and so on.
    - Thisextendedversionisknownas**MIME**(MultipurposeMailExtension).

## SIMPLEMAILTRANSFERPROTOCOL(SMTP)

* + SMTP is the standard protocol for transferring mail between hosts in the TCP/IP protocol suite.
  + SMTPisnotconcernedwiththeformatorcontentofmessagesthemselves.
  + SMTP uses information written on the *envelope* of the mail (message header), but does not look at the *contents* (message body) of the envelope.



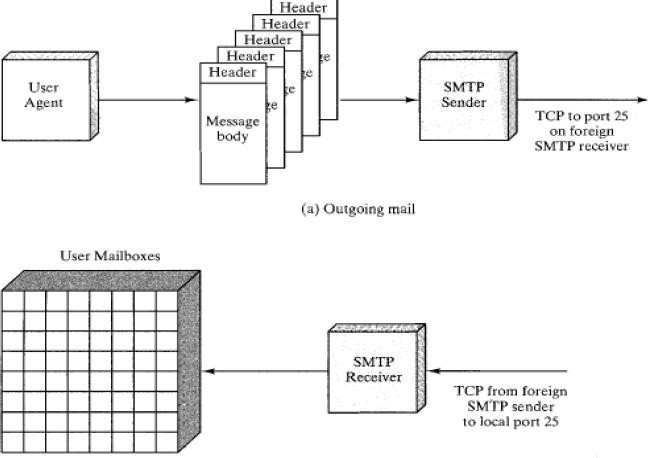
* + SMTPclientsandservershavetwomaincomponents
* **UserAgents(UA)**–Preparesthemessage,enclosesitinanenvelope.
* **MailTransferAgent(MTA)**–Transfersthemailacrosstheinternet



* + SMTPalsoallowstheuseofRelaysallowingotherMTAstorelaythemail.



### SMTPMAILFLOW

****

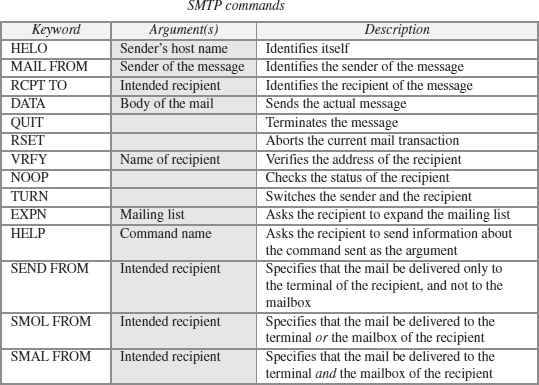
* + Tobegin,mailiscreatedbyauser-agentprograminresponsetouserinput.
  + Each created message consists of a header that includes the recipient's email address and other information, and a message body containing the message to be sent.
  + These messages are then queued in some fashion and provided as input to an SMTP Sender program.

### SMTPCOMMANDSANDRESPONSES

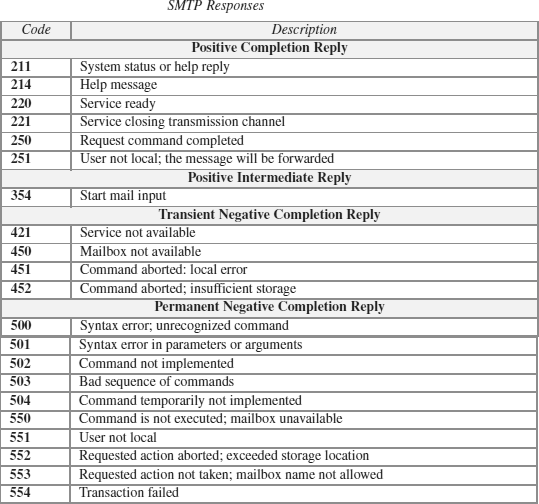
* + The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and SMTP receiver.
  + TheinitiativeiswiththeSMTPsender,whoestablishestheTCPconnection.
  + Oncetheconnectionisestablished,theSMTP sendersendscommandsoverthe connection to the receiver.
  + ThecommandisfromanMTAclienttoanMTAserver;theresponseisfrom an MTA server to the MTA client.

#### SMTPCommands

* + Commandsaresentfromtheclienttotheserver.Itconsistsofakeyword followed by zero or more arguments. SMTP defines 14 commands.



#### SMTPResponses

* + Responsesaresentfromtheservertotheclient.
  + Aresponseisathreedigitcodethatmaybefollowedbyadditionaltextual information.

### SMTPOPERATIONS

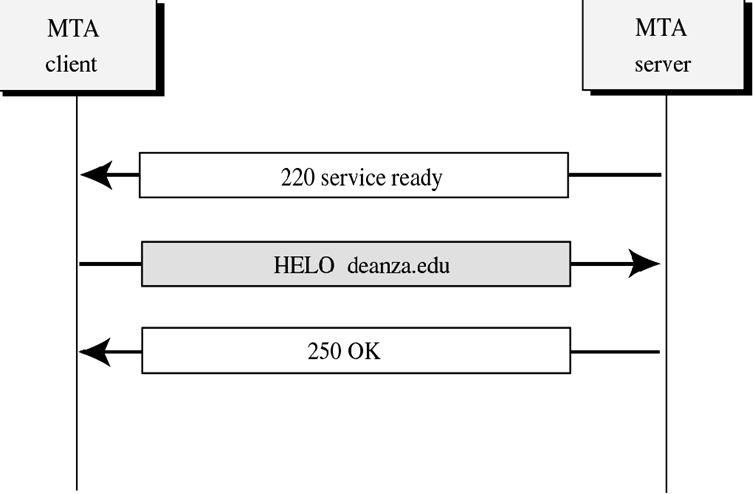
BasicSMTPoperationoccursinthreephases:

1. ConnectionSetup
2. MailTransfer
3. ConnectionTermination

#### ConnectionSetup

* + AnSMTPsenderwillattempttosetupaTCPconnectionwithatargethost when it has one or more mail messages to deliver to that host.
  + Thesequenceisquitesimple:

1. ThesenderopensaTCPconnectionwiththereceiver.
2. Oncetheconnectionisestablished,thereceiveridentifiesitselfwith "Service Ready”.
3. ThesenderidentifiesitselfwiththeHELOcommand.
4. Thereceiveracceptsthesender'sidentificationwith"OK".
5. Ifthemailserviceonthedestinationisunavailable,thedestinationhost returns a "Service Not Available" reply in step 2, and the process is terminated.



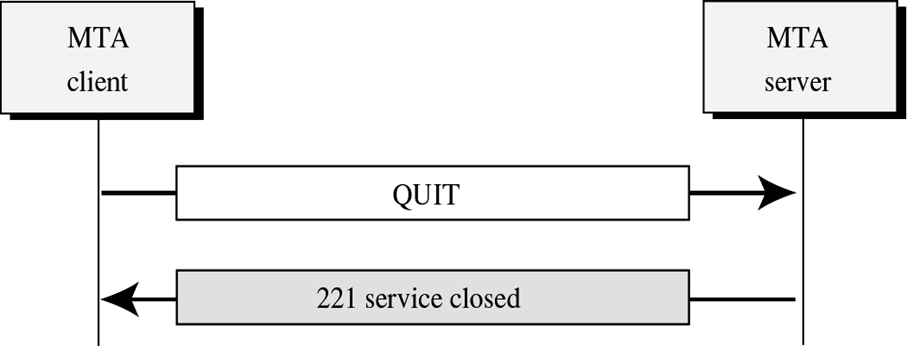
#### Mail Transfer

* + Onceaconnectionhasbeenestablished,theSMTPsendermaysendoneor more messages to the SMTP receiver.
  + Therearethreelogicalphasestothetransferofamessage:

1. AMAILcommandidentifiestheoriginatorofthemessage.
2. OneormoreRCPTcommandsidentifytherecipientsforthis message.
3. ADATAcommandtransfersthemessagetext.

#### ConnectionTermination

* + TheSMTPsenderclosestheconnectionintwosteps.
  + First,thesendersendsaQUITcommandandwaitsforareply.
  + ThesecondstepistoinitiateaTCPcloseoperationfortheTCPconnection.
  + The receiver initiates its TCP close after sending its reply to the QUIT command.



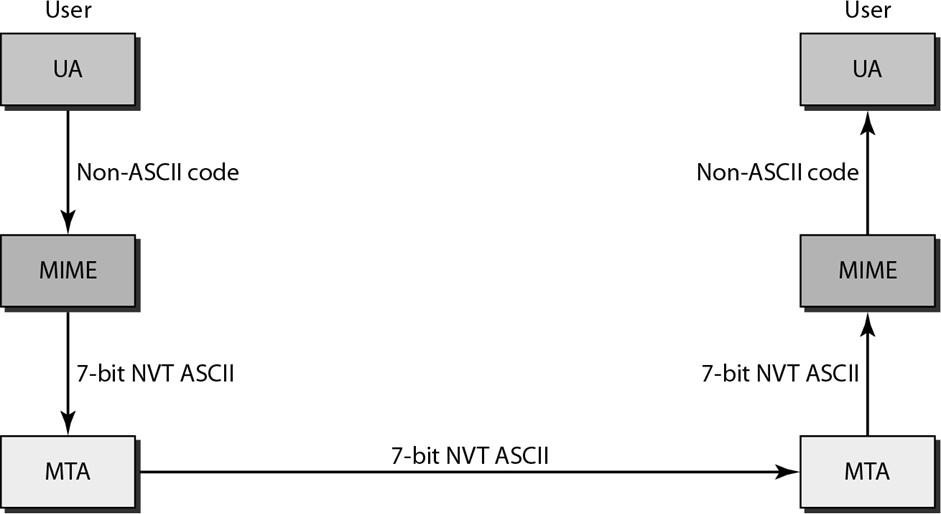
LIMITATIONSOFSMTP

* + SMTPcannottransmitexecutablefilesorotherbinaryobjects.
  + SMTP cannot transmit text data that includes national language characters, as these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
  + SMTPserversmayrejectmailmessageoveracertainsize.
  + SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
  + Some SMTPimplementationsdonotadherecompletelytothe SMTPstandards defined.
  + Commonproblemsincludethefollowing:

1. Deletion,addition,orrecordingofcarriagereturnandlinefeed.
2. Truncatingorwrappinglineslongerthan76characters.
3. Removaloftrailingwhitespace(tabandspacecharacters).
4. Paddingoflinesinamessagetothesamelength.
5. Conversionoftabcharactersintomultiple-spacecharacters.

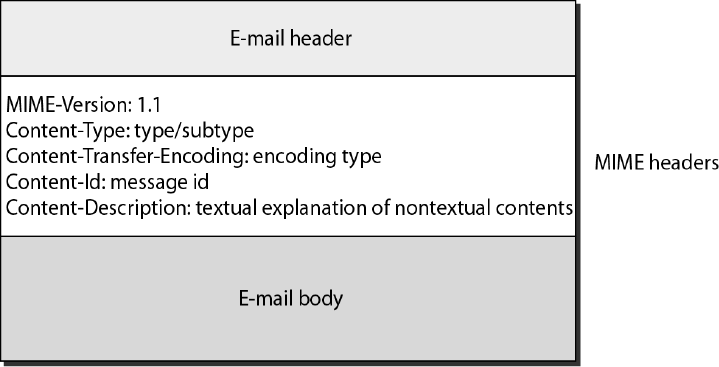
## MULTIPURPOSEINTERNETMAILEXTENSION(MIME)

* + SMTPprovidesabasicemailservice,whileMIMEaddsmultimediacapabilityto SMTP.
  + MIMEisanextensiontoSMTPandisusedtoovercometheproblemsand limitations of SMTP.
  + Emailsystemwasdesignedtosendmessagesonlyin*ASCII*format.
* LanguagessuchasFrench,Chinese,etc.,arenotsupported.
* Image,audioandvideofilescannotbesent.
  + MIMEaddsthefollowingfeaturestoemailservice:
* Beabletosendmultipleattachmentswithasinglemessage;
* Unlimitedmessagelength;
* UseofcharactersetsotherthanASCIIcode;
* Useofrichtext(layouts,fonts,colors,etc)
* Binaryattachments(executables,images, audioorvideofiles,etc.),which may bedivided if needed.
  + MIME is a protocol that *converts* non-ASCIIdata to 7-bit NVT(Network Virtual Terminal) ASCII and vice-versa.

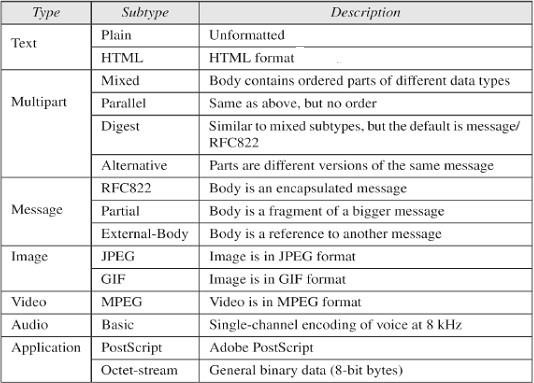


MIMEHEADERS

* + Using headers, MIME describes the type of message content and the encoding used.
  + *Headers*definedinMIMEare:
* MIME-Version-currentversion,i.e.,1.1
* Content-Type-messagetype(text/html,image/jpeg,application/pdf)
* Content-Transfer-Encoding-messageencodingscheme(egbase64).
* Content-Id-uniqueidentifierforthemessage.
* Content-Description-describestypeofthemessagebody.



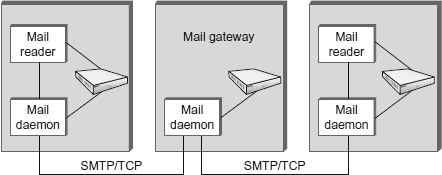
MIMECONTENTTYPES

* + Therearesevendifferentmajortypesofcontentandatotalof14subtypes.
  + Ingeneral,acontenttypedeclaresthegeneraltypeofdata,andthesubtype specifies a particular format for that type of data.
  + MIMEalsodefinesamultiparttypethatsayshowamessagecarryingmore than one data type is structured.
  + This is like a programminglanguage that defines both base types (e.g., integers and floats) and compound types (e.g., structures and arrays).
  + One possible multipart subtype is mixed, which says that the message contains a set of independent data pieces in a specified order.
  + Eachpiecethenhasitsownheaderlinethatdescribesthetypeofthatpiece.
  + ThetablebelowliststheMIMEcontenttypes:

ENCODINGFORMATSOFMIME

* + MIMEusesvariousencodingformatstoconvertbinarydataintotheASCII character set.
  + To transfer binary data, MIME offers five encodingformats which can be used in the header transfer-encoding:
* ***7-bit***:7-bittextformat(formessageswithoutaccentedcharacters);
* ***8-bit***:8-bittextformat;
* ***quoted-printable***:Quoted-Printableformat,recommendedformessages which use a7-bit alphabet (suchas when there are accent marks);
* ***base-64***:Base64,forsendingbinaryfilesasattachments;
* ***binary***:binaryformat;notrecommended.
  + SinceMIMEisveryopen,itcanusethird-partyencodingformatssuch as:
* ***BinHex***:Aproprietaryformatbelongingto Apple
* ***Uuencode***:forUNIX-to-UNIXencoding
* ***Xencode***:forbinary-to-textencoding

MESSAGETRANSFERINMIME

****

* + MTAisamaildaemon(sendmail)activeonhostshavingmailbox,usedtosend an email.
  + Mailpassesthroughasequenceof*gateways*beforeitreachestherecipient mail server.
  + Each gateway stores and forwards the mail using Simple mail transfer protocol (SMTP).
  + SMTPdefinescommunicationbetweenMTAsoverTCPonport25.
  + InanSMTPsession,sendingMTAis*client*andreceiveris*server*.Ineach exchange:
  + Clientpostsacommand(HELO,MAIL,RCPT,DATA,QUIT,VRFY,etc.)
  + Serverrespondswithacode(250,550,354,221,251etc)andanexplanation.
  + ClientisidentifiedusingHELOcommandandverifiedbytheserver
  + Clientforwardsmessagetoserver,ifserveriswillingtoaccept.
  + Messageisterminatedbyalinewithonlysingleperiod(.)init.
  + Eventuallyclientterminatestheconnection.

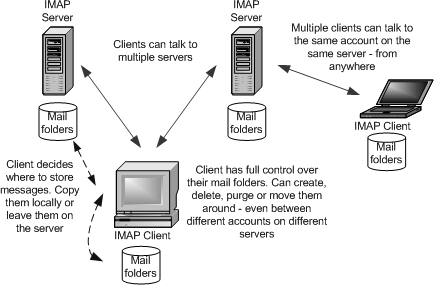
## IMAP(INTERNETMAILACCESSPROTOCOL)

* + IMAP is an Application Layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
  + It is a method of accessingelectronic mail messages that are kept on a possibly shared mail server.
  + IMAPisamorecapablewireprotocol.
  + IMAPissimilartoSMTPinmanyways.
  + IMAPisaclient/serverprotocolrunningover TCPonport143.
  + IMAP allows multiple clients simultaneously connected to the same mailbox, and through flags stored on the server, different clients accessing the same mailbox at the same or different times can detect state changes made by other clients.
  + In other words, it permits a "client" email program to access remote message stores as if they were local.
  + For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and anotebook computer while travelling, without the need to transfer messages or files back and forth between these computers.
  + IMAPcansupportemailservinginthreemodes:
* Offline
* ***Online***

Users may connect to the server, look at what email is available, and access it online. This looks to the user very much like having local spool files, but they’re on the mail server.

* Disconnectedoperation

A mail client connects to the server, can make a “cache” copy of selected messages, and disconnects from the server. The user can then workon the messages offline, and connect to the server later and resynchronize the server status with the cache.



OPERATIONOFIMAP

* + The mail transfer begins with the client authenticating the user and identifying the mailbox theywant to access.
  + ClientCommands

LOGIN,AUTHENTICATE,SELECT,EXAMINE,CLOSE,andLOGOUT

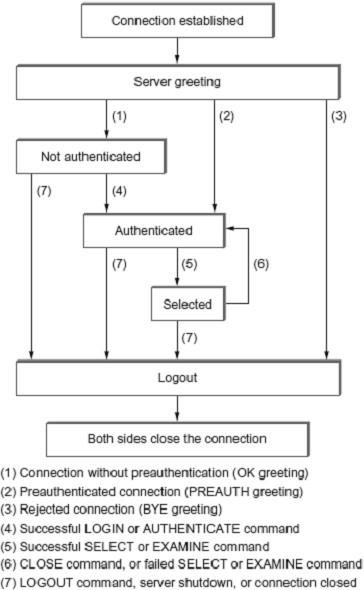
* + ServerResponses

OK,NO(nopermission),BAD(incorrectcommand),

* + WhenuserwishestoFETCHamessage,serverrespondsinMIMEformat.
  + Message*attributes*suchassizearealsoexchanged.
  + *Flags* are used by client to report user actions. SEEN,ANSWERED,DELETED,RECENT

IMAP4

* + ThelatestversionisIMAP4.IMAP4ismorepowerfulandmorecomplex.
  + IMAP4providesthefollowingextrafunctions:
* Ausercancheckthee-mailheaderpriortodownloading.
* A user can search the contents of the e-mail for a specific string of characters prior to downloading.
* Auser can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
* Ausercancreate,delete,orrenamemailboxes onthemailserver.
* Ausercancreateahierarchyofmailboxesinafolderfore-mailstorage.

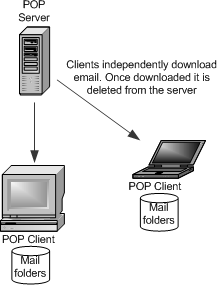


ADVANTAGESOFIMAP

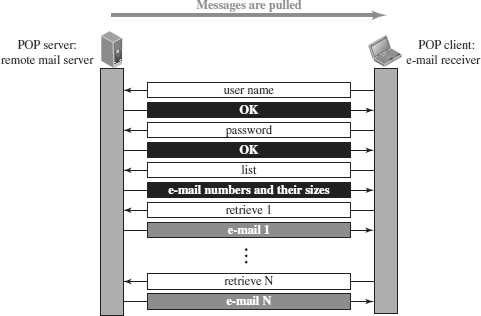
* + WithIMAP,theprimarystorageisontheserver,notonthelocalmachine.
  + Emailbeingputawayforstoragecanbefolderedonlocaldisk,orcanbe foldered on the IMAP server.
  + Theprotocolallowsfulluserofremotefolders,includingaremotefolder hierarchy and multiple inboxes.
  + Itkeepstrackofexplicitstatusofmessages,andallowsforuser-definedstatus*.*
  + Supportsnewmailnotificationexplicitly.
  + Extensiblefornon-emaildata,likenetnews,documentstorage,etc.
  + SelectivefetchingofindividualMIMEbodyparts.
  + Server-basedsearchtominimizedatatransfer.
  + Serversmayhaveextensionsthatcanbenegotiated.

**POSTOFFICEPROTOCOL(POP3)**

* + Post Office Protocol (POP3) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
  + Therearetwoversionsof POP.
* The first, called *POP2,* became a standard in the mid-80's and requires SMTP to send messages.
* The current version, POP3, can be used with or without SMTP. POP3 uses TCP/IP port 110.
  + POPisamuchsimplerprotocol,makingimplementationeasier.
  + POP supports offline access to the messages, thus requires less internet usage time
  + POPdoesnotallowsearchfacility.
  + Inordertoaccessthemessages,itisnecessarytodownloadthem.
  + Itallowsonlyonemailboxtobecreatedonserver.
  + Itisnotsuitableforaccessingnonmaildata.
  + POP mail moves the message from the email server onto the local computer, although there is usually an option to leave the messages on the email server as well.
  + POPtreatsthemailboxasonestore,andhasnoconceptoffolders.
  + POPworksintwomodesnamely,***delete*and*keep***mode.
* In ***delete mode***, mail is *deleted* from the mailbox after retrieval. The delete mode is normally used when the user is working at their permanent computer and can save and organize the received mail after reading or replying.
* In ***keep mode***, mail after reading is *kept* in mailbox for later retrieval. The keep mode is normally used when the user accesses her mail away from theirprimary computer .



* + POP3 client is *installed* on the recipient computer and POP server on the mail server.
  + Client*opens*aconnectiontotheserverusingTCPonport110.
  + Clientsendsusernameandpasswordto*access*mailboxandtoretrieve messages.



POP3Commands

POPcommandsaregenerallyabbreviatedinto codesofthreeorfourletters The followingdescribes some of the POP commands:

1. **UID-**Thiscommandopenstheconnection
2. **STAT-**Itisusedtodisplaynumberofmessagescurrentlyinthemailbox
3. **LIST-**Itisusedtogetthesummaryofmessages
4. **RETR-**Thiscommandhelpstoselectamailboxtoaccessthemessages
5. **DELE-**Itisusedtodeleteamessage
6. **RSET-**Itisusedtoresetthesessiontoitsinitialstate
7. **QUIT-**Itisusedtologoffthesession

|  |  |  |  |
| --- | --- | --- | --- |
| **DIFFERENCEBETWEENPOPANDIMAP** | | |  |
| **SNo.** | **POP** | **IMAP** | |
| 1 | Generally used to support single  client. | Designedtohandlemultipleclients. | |
| 2 | Messagesareaccessedoffline. | Messages are accessed online althoughitalsosupportsofflinemode. | |
| 3 | POPdoesnotallowsearchfacility. | IMAPoffersabilitytosearchemails. | |
| 4 | All the messages have to be  downloaded. | Itallowsselectivetransferofmessagesto  theclient. | |
| 5 | Onlyonemailboxcanbecreatedon  theserver. | Multiplemailboxescanbecreatedonthe  server. | |
| 6 | Notsuitableforaccessingnon-mail data. | Suitableforaccessingnon-maildatai.e. attachment. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | POP commands are generally abbreviatedintocodesofthreeorfour letters. Eg. STAT. | | | | IMAPcommandsarenot abbreviated, they are full. Eg. STATUS. | | | |
| 8 | It requires minimum use of server resources. | | | | Clientsaretotallydependentonserver. | | | |
| 9 | Mailsoncedownloadedcannotbe accessed from some other location. | | | | Allows mails to  multiplelocations. | be | accessed | from |
| 10 | The e-mails  automatically. | are | not | downloaded | Userscanviewtheheadingsandsender  ofe-mailsandthendecidetodownload. | | | |
| 11 | POPrequireslessinternetusagetime. | | | | IMAPrequiresmoreinternetusagetime. | | | |

AdvantagesofIMAPover POP

* + IMAPismorepowerfulandmorecomplexthanPOP.
  + Usercan*check*thee-mailheaderpriortodownloading.
  + Usercan*search*e-mailforaspecificstringofcharacterspriortodownloading.
  + Usercandownload*partially,*veryusefulincaseoflimitedbandwidth.
  + Usercancreate,delete,orrename*mailboxes*onthemailserver.

**6. TELNET(TERMINALNETWORK)**

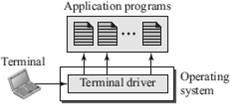
* TELNET is the original remote logging protocol, based on client-serverprogram.
* Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.
* TELNET allows us to explain the issues and challenges related to the concept of remote logging.
* Network administrators often use TELNET for diagnostic and debugging purposes.
* TELNETrequiresaloggingnameandpassword.
* It is vulnerable to hacking because it sends all data including the password inplaintext (not encrypted).
* Ahacker can eavesdrop and obtain the loggingname and password.Because of this security issue, the use of TELNET has diminished.

TYPESOFTELNETLOGGING

TherearetwotypesofTELNET logging:

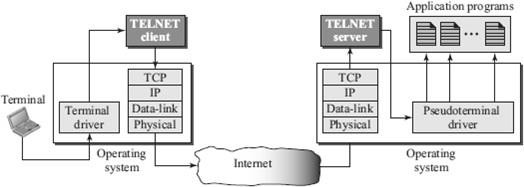
LocalLoggingandRemoteLogging

#### LocalLogin

****

* Whenauserlogsintoalocalsystem,itiscalledlocallogging.
* As a user types at a terminal or at a workstation running a terminal emulator,the keystrokes are accepted by the terminal driver.
* Theterminaldriverpassesthecharacterstotheoperatingsystem.
* Theoperatingsystem,inturn,interpretsthecombinationofcharactersand invokes the desired application program or utility.

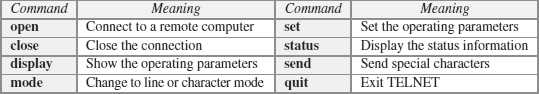
RemoteLogging

****

* When a user wants to access an application program or utility located on a remote machine, they perform remote logging.
* RemoteLoggingusesTELNETclientandTELENTserverprograms.
* The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.
* The characters are sent to the TELNET client, which transforms the characters into a universal character set called Network Virtual Terminal(NVT) characters and delivers them to the local TCP/IP stack.
* The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine.
* The characters are delivered to the operating system and passed totheTELNET server, which changes the characters to the corresponding characters understandable by the remote computer.
* The characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server; it is designed to receive characters from a terminal driver.
* A piece of software called pseudoterminal driver, is added to this,which pretends that the characters are coming from a terminal.
* The operating system then passes the characters to the appropriate application program.

TELENTOPTIONS

* TELNET lets the clientandserver negotiate options before or duringthe useof the service.
* Options are extra features available to a user with a more sophisticated terminal.
* Userswithsimplerterminalscanusedefaultfeatures.

TELENTCOMMANDS

**NETWORKVIRTUALTERMINAL(NVT)**

* Themechanismtoaccessaremotecomputeriscomplex.
* Wearedealingwithheterogeneoussystems.
* This is because every computer and its operating system accepts a special combination of characters as tokens.
* For example, the end-of-file token in a computer running the DOS operating system is Ctrl+z, while the UNIX operating system recognizes Ctrl+d.
* If we want to access any remote computer in the world, we must first know what type of computer we will be connected to, and we must also install the specific terminal emulator used by that computer.
* TELNET solves this problem by defining a universal interface called the Network Virtual Terminal (NVT) character set.
* Via this interface, theclient TELNET translates characters (dataor commands) that come from the local terminal into NVT form and delivers them to the network.
* The server TELNET, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.



#### NVTCharacterFormat

* NVTusestwosetsofcharacters,onefordataandonefor control.
* For data, NVT normally uses what is called NVT ASCII. This is an 8-bit character set in which the seven lowest order bits are the same asASCII andthe highest order bit is 0.
* To send control characters between computers , NVT uses an 8-bit characterset in which the highest order bit is set to 1.



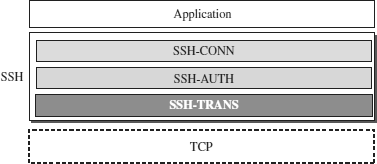
**7. SSH(SECURESHELL)**

* **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: SSH-1 and SSH-2, which are totally incompatible. The first version, SSH-1, is now deprecated because of security flaws in it.

### SSHCOMPONENTS

SSHisanapplication-layerprotocolwiththreecomponents:

1. SSHTransport-LayerProtocol(SSH-TRANS)
2. SSHAuthenticationProtocol(SSH-AUTH)
3. SSHConnectionProtocol(SSH-CONN)



#### SSHTransport-LayerProtocol(SSH-TRANS)

* + SSHfirstusesaprotocolthatcreatesasecuredchannelontopoftheTCP.
  + ThisnewlayerisanindependentprotocolreferredtoasSSH-TRANS.
  + When the procedure implementing this protocol is called, the client and server first use the TCP protocol to establish an insecure connection.
  + Then they exchange several security parameters to establish a secure channelon top of the TCP.

Servicesprovidedbythisprotocol:

1. Privacyorconfidentialityofthemessageexchanged
2. Data integrity, which means that it is guaranteed that the messages exchangedbetweentheclientandserverarenotchangedbyanintruder
3. Serverauthentication,whichmeansthattheclientisnowsurethattheserver is the one that it claims to be
4. Compressionofthemessages,whichimprovestheefficiencyofthesystem and makes attack more difficult

#### SSHAuthenticationProtocol(SSH-AUTH)

* + After a secure channel is established between the client and the server and the server is authenticated for the client.
  + SSHcancallanotherprocedurethatcanauthenticatetheclientfortheserver.
  + This layer defines a number of authentication tools similar to the ones used in SSL.
  + Authentication starts with the client, which sends a request message to the server.
  + The request includesthe username, server name, the method of authentication, and the required data.
  + The server responds with either a success message, which confirms that the client is authenticated, or a failed message, which means that the process needs to be repeated with a new request message.

#### SSHConnectionProtocol(SSH-CONN)

* + After the secured channel is established and both server and client are authenticated for each other, SSH can call a piece of software that implements the third protocol, SSHCONN.
  + OneoftheservicesprovidedbytheSSH-CONNprotocolismultiplexing.
  + SSH-CONN takes the secure channel established by the two previous protocols and lets the client create multiple logical channels over it.
  + Each channel can be used for a different purpose, such as remote logging, file transfer, and so on.

### SSHAPPLICATIONS

SSH is a general-purpose protocol that provides a secure connection between a client and server.

#### SSHforRemoteLogging

* + SeveralfreeandcommercialapplicationsuseSSHforremotelogging.
  + Amongthem,wecanmentionPuTTy,bySimonTatham,whichisaclientSSH program that can beused for remote logging.
  + AnotherapplicationprogramisTectia,whichcanbeusedonseveralplatforms.

#### SSHforFileTransfer

* + One of the application programs that is built on top of SSH for file transfer is the *Secure File Transfer Program* (*sftp*).
  + The *sftp* application program uses one of the channels provided by the SSH to transfer files.
  + Anothercommonapplicationiscalled*SecureCopy*(*scp*).
  + This application uses thesame formatas the UNIX copy command, *cp,*to copy files.

#### PortForwarding

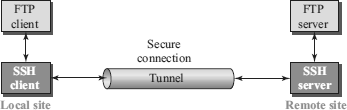
* + OneoftheinterestingservicesprovidedbytheSSHprotocolisport forwarding.
  + WecanusethesecuredchannelsavailableinSSHtoaccessanapplication program that does not provide security services.
  + Applications such as TELNET and Simple Mail Transfer Protocol (SMTP),can use the services of the SSH port forwarding mechanism.
  + The SSH port forwarding mechanism creates a tunnel through which the messages belonging to other protocols can travel.
  + Forthisreason,thismechanismissometimesreferredtoasSSH*tunneling*.

### SSHPACKETFORMAT

****

* + Thelengthfielddefinesthelengthofthepacketbutdoesnotincludethepadding.
  + ThePaddingfieldisaddedtothepackettomaketheattackonthesecurity provision more difficult.
  + The type field designates the type of the packet used in different SSHprotocols.
  + Thedatafieldisthedatatransferredbythepacketindifferentprotocols.
  + TheCRCfieldisusedforerror detection.

### SECURINGFTPAPPLICATIONSUSINGSSH

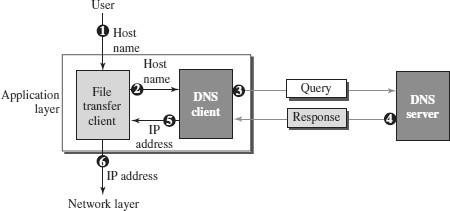
****

* + TheFTPclientcanusetheSSHclientonthelocalsitetomakeasecure connection
  + withtheSSHserverontheremotesite.
  + Any request fromthe FTP client to theFTP server is carried through the tunnel provided by the SSH client and server.
  + Any response from the FTP server to the FTP client is also carried through the tunnel provided by the SSH client and server.

**8. DNS(DOMAINNAMESYSTEM)**

* DomainNameSystemwasdesignedin1984.
* DNSisusedforname-to-addressmapping.
* The DNS provides the protocol which allows clients and servers to communicate with each other.
* Eg: Host name like [www.yahoo.com](http://www.yahoo.com/) is translated into numerical IP addresses like 207.174.77.131
* Domain Name System (DNS) is a distributed database used by TCP/IP applications to map between hostnames and IP addresses and to provide electronic mail routing information.
* Each site maintains its own database of information and runs a server program that other systems across the Internet can query.

WORKINGOFDNS

****

The following six steps shows the working of a DNS. It maps the host name to an IP address:

1. Theuserpassesthehostnametothefiletransferclient.
2. ThefiletransferclientpassesthehostnametotheDNSclient.
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. TheDNSserverrespondswiththeIPaddressofthedesiredfiletransferserver.
5. TheDNSserverpassestheIPaddresstothefiletransferclient.
6. The file transfer client now uses the received IP address to access the file transfer server.

NAMESPACE

* + Tobeunambiguous,thenamesassignedto machinesmustbecarefullyselected from a name space with complete control over the binding between the names and IP address.
  + Thenamesmustbeuniquebecausetheaddressesareunique.
  + Anamespacethatmapseachaddresstoauniquenamecanbeorganizedin two ways: ***flat(*or)*hierarchical*.**

**FlatNameSpace**

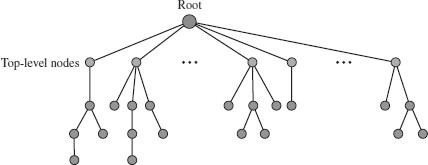
* Inaflatnamespace,anameisassignedtoanaddress.
* Anameinthisspaceisasequenceofcharacterswithoutstructure.
* Themaindisadvantageofaflatnamespaceisthatitcannotbeusedina large system such as Internet because it must be centrally controlled to avoid ambiguity and duplication.

**HierarchicalNameSpace**

* Inahierarchicalnamespace,eachnameismadeofseveralparts.
* The first part can define the organization, the second part can define the name, the third part can define departments, and so on.
* Inthiscase,theauthoritytoassignandcontrolthenamespacescanbe decentralized.
* Acentralauthoritycanassignthepartofthenamethatdefinesthenatureofthe organization and the name.
* Theresponsibilityfortherestofthenamecanbegiventotheorganization itself. Suffixes can be added to the name to define host or resources.
* The management of the organization need not worry that the prefix chosen fora host is taken by another organization because even if part of an address is the same, the whole address is different.
* Thenamesareuniquewithouttheneedtobeassignedbyacentralauthority.
* Thecentralauthoritycontrolsonlypartofthename,notthewholename.

DOMAINNAMESPACE

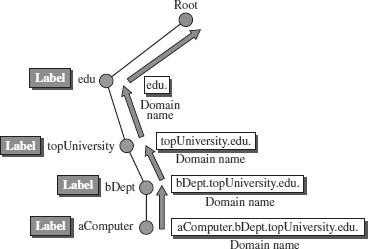
* + To have a hierarchical name space, a domain name space was designed. In this design, the names are defined in an inverted-tree structure with the root at the top.
  + Each node in the tree has a label, which is a string with a maximum of 63 characters.
  + Therootlabelisanullstring.
  + DNS requires that children of a node have different labels, which guaranteesthe uniqueness of the domain names.



* + Each node in the tree has a **label**, which is a string with a maximum of 63 characters.
  + The root label is a null string (empty string). DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

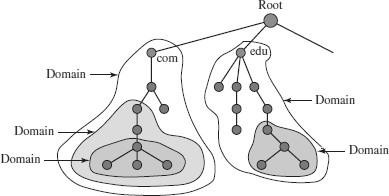
DomainName

* + - Eachnodeinthetreehasalabelcalledasdomainname.
    - Afulldomainnameisasequenceoflabelsseparatedbydots (**.**)
    - Thedomainnamesarealwaysreadfromthenodeuptotheroot.
    - Thelastlabelisthelabeloftheroot(null).
    - Thismeansthatafulldomainnamealwaysendsinanulllabel,which means the last character is a dot because the null string is nothing.
    - Ifalabelisterminatedbyanullstring,itiscalleda ***fullyqualifieddomain name (FQDN)****.*
    - Ifalabelisnotterminatedbyanullstring,itiscalleda ***partiallyqualified domain name (PQDN).***

******

Domain

* Adomainisasubtreeofthedomainnamespace.
* Thenameofthedomainisthedomainnameofthenodeatthetopofthesub- tree.
* Adomainmayitselfbedividedintodomains.

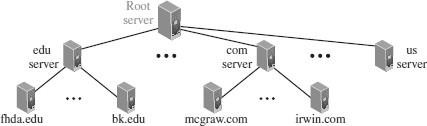


DISTRIBUTIONOFNAMESPACE

* + Theinformationcontainedinthedomainnamespacemustbestored.
  + But it is very inefficient and also not reliable to have just one computer storesuch a huge amount of information.
  + Itis inefficient because respondingto requestsfromall over the world, placesa heavy load on the system.
  + Itisnotreliablebecauseanyfailuremakesthedatainaccessible.
  + Thesolutiontotheseproblemsistodistributetheinformationamongmany computers called ***DNS servers***.

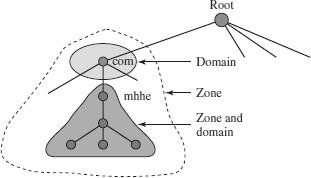
HIERARCHYOFNAMESERVERS

* + The way to distribute information among DNS serversis to divide the wholespace into many domains based on the first level.
  + Lettherootstand-aloneandcreateasmanydomainsastherearefirstlevel nodes.
  + Becauseadomaincreatedthiswaycouldbeverylarge,
  + DNSallowsdomainstobedividedfurtherintosmallerdomains.
  + Thus we have a hierarchy of servers in the same way that we have a hierarchy of names.



ZONE

* + Whataserverisresponsiblefor,orhasauthorityover,iscalleda***zone***.
  + The server makes a database called a *zone* fileand keeps all the information for every node under that domain.
  + If a server accepts responsibility for a domain and does not divide the domains into smaller domains, the domain and zone refer to the same thing.
  + But if a server divides its domain into sub domains and delegates parts of its authority to other servers, domain and zone refer to different things.
  + The information about the nodes in the sub domains is stored in the servers at the lower levels, with the original server keeping some sort of references to these lower level servers.
  + Butstill,theoriginalserverdoesnotfreeitselffromresponsibilitytotally.
  + It still has a zone, but the detailed information is kept by the lower levelservers.



ROOTSERVER

* + Arootseverisaserverwhosezoneconsistsofthewholetree.
  + A root server usually does not store any information about domains but delegatesitsauthoritytootherservers,keepingreferencestothoseservers.
  + Currently there are more than 13 root servers, each coveringthe whole domain name space.
  + Theserversaredistributedallaroundtheworld.

PRIMARYANDSECONDARYSERVERS

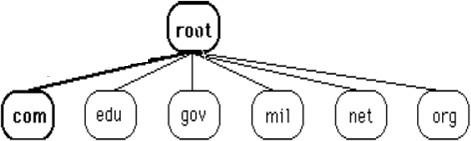
* + DNSdefinestwotypesofservers:primaryandsecondary.
  + A Primary Server is a server that stores a file about the zone for which it is an authority.
    - Primary Servers are responsible for creating, maintaining, and updating the zone file.
    - PrimaryServerstoresthezonefileonalocaldisc.
  + A secondary server is a server that transfers the complete information about a zone fromanother server (Primary or Secondary) and stores the file on its local disc.
  + If updating is required, it must be done by the primary server, which sends the updated version to the secondary.
  + A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

DNSINTHEINTERNET

* + DNSisaprotocolthatcanbeusedindifferentplatforms.
  + IntheInternet,thedomainnamespace(tree)isdividedintothreedifferent sections -***Generic domains,Country domains, andInverse domain***.

**GenericDomains**

* + Thegenericdomainsdefineregisteredhostsaccordingtotheirgeneric behavior.
  + Each node in the tree defines a domain, which is an index to the domain name space database.
  + Thefirstlevelinthe genericdomainssectionallowssevenpossiblethree character levels.
  + Theselevelsdescribetheorganizationtypesaslistedinfollowingtable**.**

****

**CountryDomains**

* + The country domains section follows the same format as the generic domainsbut uses two characters for country abbreviations
  + E.g.;***in***for***India***,***us***for***UnitedStates***etc)inplaceofthethreecharacter organizational abbreviation at the first level.
  + Second level labels can be organizational, or they can be more specific, national designation.
  + Indiaforexample,usesstateabbreviationsasasubdivisionofthecountry domain us. (e.g., ca.in.)

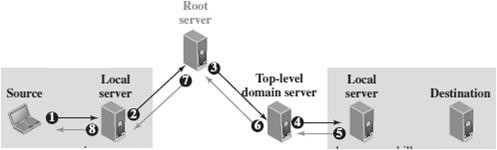
**InverseDomains**

* + MappinganaddresstoanameiscalledInversedomain.
  + The client can send an IP address to a server to be mapped to a domain name and it is called *PTR(Pointer)query*.
  + Toanswerqueriesofthiskind,DNSusestheinverse domain

DNSRESOLUTION

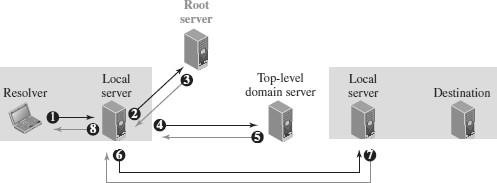
* + Mapping a name to an address or an address to a name is called name address resolution.
  + DNSisdesignedasaclientserverapplication.
  + A host that needs to map an address to a name or a name to an address calls a DNS client named a ***Resolver***.
  + TheResolveraccessestheclosestDNSserverwithamappingrequest.
  + If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.
  + Aftertheresolverreceivesthe mapping,itinterprets theresponsetoseeifitisa real resolution or an error and finally delivers the result to the process that requested it.
  + Aresolutioncanbeeither***recursiveoriterative***.

**RecursiveResolution**

****

* The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host. The resolver, which does not know this address, sends the query to the localDNSserver of the source (Event 1)
* ThelocalserversendsthequerytoarootDNSserver(Event 2)
* TheRootserversendsthequerytothetop-level-DNSserver(Event3)
* The top-level DNSserver knows only the IP address of the local DNSserver at the destination. So itforwards thequeryto thelocal server, which knows the IP address of the destination host (Event 4)
* The IP address of the destination host is now sent back to the top-level DNS server(Event 5) then back to the root server (Event 6), then back to the source DNS server, which may cache it for the future queries (Event 7), and finally back to the source host (Event 8).

**IterativeResolution**

****

* In iterative resolution**,** each server that does not know the mapping, sends theIP address of the next server back to the one that requested it.
* Theiterativeresolutiontakesplacebetweentwolocalservers.
* Theoriginalresolvergetsthefinalanswerfromthedestinationlocalserver.
* ThemessagesshownbyEvents2,4,and6containthesamequery.
* However,themessageshownbyEvent3containstheIPaddressofthetop- level domain server.
* The message shown by Event 5 contains the IP address of the destination local DNS server
* ThemessageshownbyEvent7containstheIPaddressofthedestination.
* When the Source local DNSserver receives the IP address of the destination, it sends it to the resolver (Event 8).

DNSCACHING

* + Eachtimeaserverreceivesaqueryforaname thatisnotinitsdomain,itneeds to search its database for a server IP address.
  + DNShandlesthiswithamechanismcalled***caching****.*
  + When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
  + If the same or another client asks for the same mapping, it can check its cache memory and resolve the problem.
  + However, to inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as ***unauthoritative****.*
  + Caching speeds up resolution. Reduction of this search time would increase efficiency,but it can also be problematic.
  + If a server caches a mapping for a long time, it may send an outdated mapping to the client.
  + Tocounterthis,twotechniquesareused.
* First, the authoritative server always adds information to the mapping called ***time to live (TTL)***. It defines the time in seconds thatthe receiving server can cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server.
* Second, DNS requires that each server keep a ***TTL counter*** for each mapping it caches. The cache memory must be searched periodicallyand those mappings with an expired TTL must be purged.

DNSRESOURCERECORDS(RR)

* Thezoneinformationassociatedwithaserverisimplementedasasetof

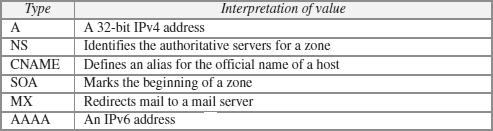
*resourcerecords*.

* Inotherwords,anameserverstoresadatabaseofresourcerecords.
* A*resourcerecord*isa5-tuplestructure :

(DomainName,Type,Class,TTL,Value)

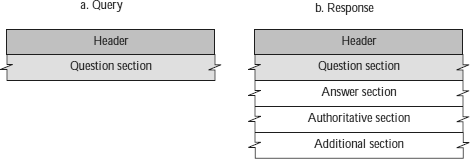
* Thedomainnameidentifiestheresourcerecord.
* Thetypedefineshowthevalueshouldbeinterpreted.
* Thevaluedefinestheinformationkeptaboutthedomainname.
* TheTTLdefinesthenumberofsecondsforwhichtheinformationisvalid.
* Theclassdefinesthe typeofnetwork

**TypesofResourceRecords**

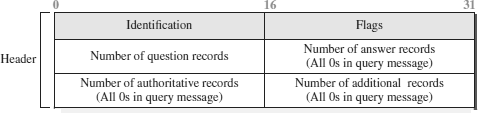
****

DNSMESSAGES

* + DNShastwotypesofmessages:queryandresponse.
  + Bothtypeshavethesameformat.
  + Thequerymessageconsistsofaheaderandquestionsection.
  + Theresponse message consistsof a header, question section,answer section, authoritative section, and additional section .



* + **Header**
    - Bothqueryandresponsemessageshavethesameheaderformatwith some fields set to zero for the query messages.
    - Theheaderfieldsareasfollows:



* + - The identification field is used by the client to match the response with the query.
    - Theflagfielddefineswhetherthe messageisaqueryorresponse.Italso includes status of error.
    - The next four fields in the header define the number of each record type in the message.
  + QuestionSection
    - Thequestionsectionconsistsofoneormorequestionrecords.Itis present in both query and response messages.
  + AnswerSection
    - The answer section consists of one or more resource records. It is present only in response messages.
  + AuthoritativeSection
    - The authoritative section gives information (domain name) about one or more authoritative servers for the query.
  + AdditionalInformationSection
    - The additional information section provides additional information that may help the resolver.

DNSCONNECTIONS

* + DNScanuseeitherUDPorTCP.
  + Inbothcasesthewell-knownportusedbytheserverisport 53.
  + UDPisusedwhenthesizeoftheresponsemessageislessthan512bytes because most UDP packages have a 512-byte packet size limit.
  + Ifthe size oftheresponse messageis morethan512 bytes, aTCP connection is used.

DNSREGISTRARS

* + NewdomainsareaddedtoDNSthrougha*registrar.*Afeeischarged.
  + Aregistrarfirstverifiesthattherequesteddomainnameisuniqueandthen enters it into the DNS database.
* Today,therearemanyregistrars;theirnamesandaddressescanbefound at

[***http://www.intenic.net***](http://www.intenic.net/)

* + Toregister,theorganizationneedstogivethenameofitsserverandtheIP address of the server.
  + Forexample,anewcommercialorganizationnamed *wonderful*withaserver named *ws* and IP address 200.200.200.5, needs to give the following information to one of the registrars:

***Domainname:****ws.wonderful.com****IPaddress:****200.200.200.5*

DDNS(DYNAMICDOMAINNAMESYSTEM)

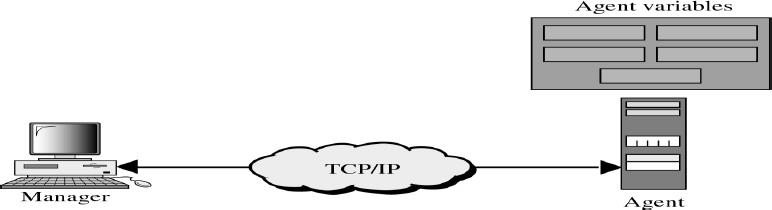
* + InDNS,whenthereisachange, suchasaddinganewhost,removingahost,or changing an IP address, the change must be made to the DNS master file.
  + TheDNSmasterfilemustbeupdateddynamically.
  + The***DynamicDomainNameSystem(DDNS)***isusedforthispurpose.
  + In DDNS, when a binding between a name and an address is determined, theinformation is sent to a primary DNS server.
  + Theprimaryserverupdatesthezone.
  + Thesecondaryserversarenotifiedeitheractivelyorpassively.
  + In active notification, the primary server sends a message to the secondary servers about the change in the zone, whereas in passive notification, the secondary servers periodically check for any changes.
  + In either case, after being notified about the change, the secondary server requests information about the entire zone (called the *zone transfer*).
  + To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

DNSSECURITY

* + DNSisoneofthemostimportantsystemsintheInternetinfrastructure;it provides crucial services to Internet users.
  + Applications such as Web access ore-mail are heavily dependent on the proper operation of DNS.
  + DNScanbeattackedinseveralwaysincluding:
    - ***Attack on Confidentiality*** - The attacker may read the response of a DNS ***server*** to find the nature or names of sites the user mostly accesses. This type of information can be used to find the user’s profile. To prevent this attack, DNS messages need to be confidential.
    - ***Attack on authentication*** and ***integrity*** - The attacker may intercept the response of a DNS server and change it or create a totally new bogus ***response*** to direct the user to the site or domain the attacker wishes the user to access. This type of attack can be prevented using message origin authentication and message integrity.
    - ***Attack on denial-of-service*** - The attacker may flood the DNS server to overwhelm it or eventually crash it. This type of attack can be prevented using the provision against denial-of-service attack***.***
  + To protect DNS, IETF has devised a technology named ***DNS Security (DNSSEC)***that***providesmessageoriginauthenticationandmessageintegrity*** using a security service called ***digital signature****.*
  + DNSSEC,however,***doesnotprovideconfidentiality***fortheDNSmessages.
  + There is ***no specific protection against the denial-of-service attack*** in the specification of DNSSEC. However, the caching system protects the upper- level servers against this attack to some extent.

**9. SNMP(SIMPLENETWORKMANAGEMENTPROTOCOL)**

* + The**SimpleNetworkManagementProtocol(SNMP)**isaframeworkfor managing devices in an internet using the TCP/IP protocol suite.
  + SNMPisanapplicationlayerprotocolthatmonitorsandmanagesrouters, distributed over a network.
  + Itprovidesasetofoperationsformonitoringandmanagingtheinternet.
  + SNMPusesservicesofUDP ontwo well-knownports: 161(Agent)and 162 (manager).
  + SNMPusestheconceptof***manager***and***agent***.



SNMPMANAGER

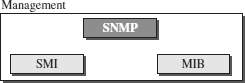
* AmanagerisahostthatrunstheSNMPclientprogram
* Themanagerhasaccesstothevaluesinthedatabasekeptbytheagent.
* Amanagercheckstheagentbyrequestingtheinformationthatreflectsthe behavior of the agent.
* Amanageralsoforcestheagenttoperformacertainfunctionbyresetting values in the agent database.
* For example, a router can store in appropriate variables the number of packets received and forwarded.
* The manager can fetch and compare the values of these two variables to see if the router is congested or not.

SNMPAGENT

* TheagentisarouterthatrunstheSNMPserver program.
* The agent is used to keep the information in a database while the manager is used to access the values in the database.
* For example, a router can store the appropriate variables such as a number of packetsreceivedandforwarded whilethemanager can compare thesevariables to determine whether the router is congested or not.
* Agentscanalsocontributetothemanagementprocess.
* A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

SNMPMANAGEMENTCOMPONENTS

* Management of the internet is achieved through simple interaction between a manager and agent.
* Managementisachievedthroughtheuseoftwoprotocols:
  + StructureofManagementInformation(SMI)
  + ManagementInformationBase(MIB).



#### StructureofManagementInformation(SMI)

* TouseSNMP,weneedrulesfornamingobjects.
* SMIisaprotocolthatdefinestheserules.
* SMIisaguidelineforSNMP
* It emphasizes three attributes to handle an object: name, data type, and encoding method.
* Itsfunctionsare:
* Tonameobjects.
* Todefinethetypeofdatathatcanbestoredinanobject.
* Toshowhowtoencodedatafortransmissionoverthenetwork.

Name

* SMIrequires that each managed object (such as a router, a variable in a router, a value,etc.) have a unique name. To name objects globally.
* SMI uses an ***object identifier*,** which is a hierarchical identifier based on a tree structure.
* Thetreestructurestartswithanunnamedroot.Eachobjectcanbedefined using a sequence of integers separated by dots.
* The tree structure can also define an object using a sequence of textual names separated by dots.

Typeofdata

* Thesecondattributeofanobjectisthetypeofdatastoredinit.
* Todefinethedatatype,SMIuses**AbstractSyntaxNotationOne(ASN.1)**

definitions.

* SMIhastwobroadcategoriesofdatatypes:*simple*and*structured.*
* The **simple data types** are atomic data types. Some of them are taken directly from ASN.1; some are added by SMI.
* SMIdefinestwo**structureddatatypes:***sequence*and*sequenceof*.
  + ***Sequence -*** A *sequence* data type is a combination of simple data types, not necessarily of the same type.
  + ***Sequence of -*** A *sequence of* data type is a combination of simple data types all of the same type or a combination of sequence data types all of the same type.

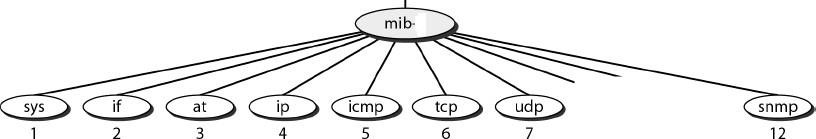
Encodingdata

* SMIuses another standard, ***Basic Encoding Rules (BER),*** to encode data to be transmitted over the network.
* BER specifies that each piece of data be encoded in triplet format (TLV): tag, length, value

#### ManagementInformationBase(MIB)

The Management Information Base (MIB) is the second component used in network management.

* EachagenthasitsownMIB, whichisa*collection*ofobjectstobemanaged.
* MIBclassifiesobjectsundergroups.



MIBVariables

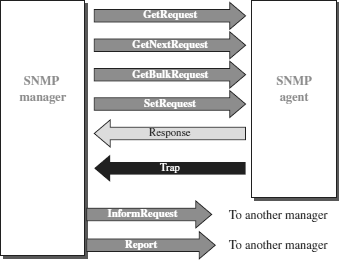
MIBvariablesareoftwotypesnamely*simple*and*table*.

* Simplevariablesareaccessedusing*group-id*followedby*variable*-*id*and0
* Tablesareorderedas*column-row*rules,i.e.,columnbycolumnfromtopto bottom. Only *leaf* elements are accessible in a table type.

SNMPMESSAGES/PDU

SNMPisrequest/replyprotocolthatsupportsvariousoperationsusingPDUs. SNMPdefines eight types of protocol data units (or PDUs):

GetRequest,GetNext-Request,GetBulkRequest,SetRequest,Response,Trap, InformRequest, and Report

******

***GetRequest***

* The GetRequest PDU is sent from the manager (client) to the agent (server) to retrieve the value of a variable or a set of variables.

GetNextRequest

* The GetNextRequest PDU is sent fromthe manager to the agent to retrieve the value of a variable.

GetBulkRequest

* The GetBulkRequest PDU is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest PDUs.

SetRequest

* TheSetRequestPDUissentfromthemanagertotheagenttoset(store)a value in a variable.

Response

* The Response PDU is sent from an agent to a manager in response to GetRequest or GetNextRequest. It contains the value(s) of the variable(s) requested by the manager.

Trap

* The Trap PDU is sent from the agent to the manager to report an event. For example,iftheagentisrebooted,itinformsthemanagerandreportsthetimeof rebooting.

InformRequest

* The InformRequest PDU is sent from one manager to another remote manager to get the value of some variables from agents under the control of the remote manager. The remote manager responds with a Response PDU.

Report

* TheReportPDUisdesignedtoreportsometypesoferrorsbetweenmanagers.