# UNIT I

**Introduction**

**Computer network** is a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they can exchange information. Neither the Internet nor the World Wide Web is a computer network. The Internet is not a single network, but a network of networks and the Web is a distributed system that runs on top of the Internet.

## Difference between a computer network and a distributed system

A distributed system consists of several systems connected that communicate with each other and share the task to be executed. This is carried by a special operating system which hides the details of execution from the user and presents them with the results as if they are executed on a single system. The user is not aware of task sharing or the systems.

In a computer network, Users are exposed to the actual machines, without any attempt by the system to hide the execution details. If the machines have different hardware and different operating systems, that is fully visible to the users. If a user wants to run a program on a remote machine, he has to log onto that machine and run it there.

The distinction between a network and a distributed system lies with the software (especially the operating system), rather than with the hardware.

* 1. **Uses of computer networks**

**1. Business Applications**

* + To be able to extract and correlate information about the entire company
  + To provide resource sharing and make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user.
  + Client server Model: In this model, the data are stored on powerful computers called servers. Often these are centrally housed and maintained by a system administrator. The employees have simpler machines, called clients, on their desks, with which they access remote data stored on servers.
  + A computer network can provide a powerful communication medium among employees like email, video conferencing, instant messenger etc
  + To do business electronically with other companies, especially suppliers and customers.
  + To business with consumers over the Internet.

**2. Home Applications**

* + Access to remote information.

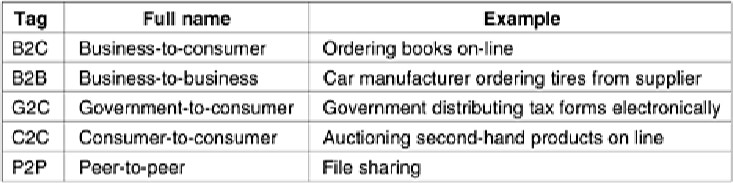
Access to remote information involves interaction· between a person and a remote database. Access to remote information comes in many forms like:

1. Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.
2. Newspaper, digital library consisting of books, magazines, scientific journals etc.
3. World Wide Web which contains information. About the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.
   * Person-to-person communication.

Email, Instant Messenger, Video Conferencing etc

* + Interactive entertainment. Interactive entertainment includes:

1. Multiperson real-time simulation games.
2. Video on demand.
3. Participation in live TV programmes likes quiz, contest, discussions etc.
   * Electronic commerce.



**3. Mobile Users**

* + Portable office
  + People on the road often want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, surf the Web, access remote files.
  + E-commerce
  + Payment Wallets
  + Video Streaming

**4. Social issues**

* + Privacy
  + Identity theft
  + Employee rights versus employer rights
  + Government versus citizen

**1.2 Network hardware**

All computer networks fit into two dimensions: transmission technology and scale.

## Based on Transmission Technology networks can be classified in two types.

1. Broadcast links. 2. Point-to-point links.
   * **Broadcast networks** have a single communication channel that is shared by all the machines on the network. Short messages, called packets in certain contexts, sent by any machine are received by all the others. An address field within the packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
   * **Point-to-point networks** consist of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks usually are point-to-point. Point-to-point transmission with one sender and one receiver is sometimes called **unicasting**.

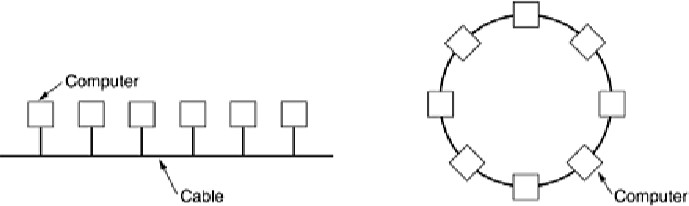
## Based on Scale networks can be classified into the following:

At the top are the personal area networks, networks that are meant for one person. Beyond the personal area networks come longer-range networks. These can be divided into local, metropolitan, and wide area networks.

## Local Area Networks

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources and exchange information. LANs are distinguished from other kinds of networks by three characteristics: (1) their size, (2) their transmission technology, and (3) their topology.

* + LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.
  + LANs may use a transmission technology consisting of a cable to which all the machines are attached.
  + Two typical topologies for LAN are bus and ring. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs.



BUS RING

## Metropolitan Area Networks

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

## Wide Area Networks

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs.

The hosts are connected by a communication subnet, or just subnet. The job of the subnet is to carry messages from host to host. Subnet consists of Transmission lines and routers. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Routers choose an outgoing line on which to forward bits. Routers adopt store and forward (Packet Switched) principle.

## Wireless Networks

wireless networks can be divided into three main categories:

1. System interconnection. 2. Wireless LANs. 3. Wireless WANs.

System interconnection is all about interconnecting the components of a computer using short-range radio. Bluetooth can be used connect components without using wires.

Wireless LANs are systems in which every computer has a radio modem and antenna with which it can communicate with other systems. Often there is an antenna on the ceiling that the machines talk to. However, if the systems are close enough, they can communicate directly with one another in a peer-to-peer configuration.

High-bandwidth wide area wireless networks are also being developed. The initial focus is high-speed wireless Internet access from homes and businesses, bypassing the telephone system. This service is often called local multipoint distribution service.

## Home Networks

The fundamental idea is that in the future most homes will be set up for networking. Every device in the home will be capable of communicating with every other device, and all of them will be accessible over the Internet. Home networking has some fundamentally different properties than other network types.

* + First, the network and devices have to be easy to install.
  + Second, the network and devices have to be foolproof in operation
  + Third, low price is essential for success.
  + Fourth, the main application is likely to involve multimedia, so the network needs sufficient capacity
  + Fifth, it must be possible to start out with one or two devices and expand the reach of the network gradually.
  + Sixth, security and reliability will be very important.

## Internetworks

A collection of interconnected networks is called an internetwork or internet.

* + Connect a collection of different LANs with in a department
  + Connect different LANs through a WAN, with WAN acting as a subnet
  + Connect different WANs to each other by means of gateways the Internet

## Network software

## Protocol Hierarchies

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are implemented.

Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed. The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one. A set of layers and protocols is called a network architecture. The specification of architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.

## Design Issues for the Layers

Some of the key design issues that occur in computer networks are present in several layers. Below, are the important ones? Every layer needs a mechanism for identifying senders and receivers.

**Rules for data transfer.**

* + Error control.
  + Data Transfer Rate
  + Mechanisms for disassembling, transmitting, and then reassembling messages.
  + Multiplexing and demultiplexing
  + Routing

**Connection-Oriented and Connectionless Services**

**Connection Oriented Services**

There is a sequence of operation to be followed by the users of connection oriented service. These are:

* + Connection is established.
  + Information is sent.
  + Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection. Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

## Connection less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received. In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

|  |  |  |
| --- | --- | --- |
| **Protocol Characteristics** | **Connection Oriented Protocol Sevices** | **Connectionless Protocol Sevices** |
| 1) Definition | It is the communication service in which  virtual connection is created before sending the packet over the internet. | In this communication service, packets are sent without creating any virtual connection over the  internet. |
| 2) Authentication | It needs authentication of the destination node before transferring data. | It transfers the data message without authenticating  destination. |
| 3) Reliability | This is a more reliable connection as it makes the virtual connection before sending packets and ensures delivery of  the packet to the destination. | This connection does not ensure reliability on packet transmission. |
| 4) Handshaking | The handshaking is carried out to ensure both sender and receiver agree with this  connection. | There is no handshaking happens while sending a packet over the  network. |
| 5) Delay | It is slower than the connectionless service. Before sending a packet, the virtual connection is created in the connection-oriented protocol which adds  extra delay. | It is faster than connection- oriented protocol service. |
| 6) Overhead | Sending packet in connection-oriented service requires more parameters in the header of the packet to ensure the reliable  transmission. | It has less overhead and smaller packet header size. |
| 7) Routing | Route is finalized and decided at the time of handshaking before sending the actual packet. | The route is not finalized and decided on the way while transferring data packet based on  the network congestion. |
| 8) Packet Travel | All the packets between sender and destination follow the same path. | Not necessary all the packets transmitting between sender and  Receiver follows the same path. |
| 9) Protocol | TCP is connection-oriented protocol. | UDP is connectionless protocol. |

## Service Primitives

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets. The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connection-less service. There are five types of service primitives:

1. LISTEN: When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.

2. CONNECT: It connects the server by establishing a connection. Response is awaited.

RECIEVE: Then the RECIEVE call blocks the server.

3. SEND: Then the client executes SEND primitive to transmit its request followed by the execution of .

4. RECIEVE to get the reply. Send the message.

5. DISCONNECT: This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

**Connection Oriented Service Primitives**

There are 5 types of primitives for Connection Oriented Service:

|  |  |
| --- | --- |
| LISTEN | Block waiting for an incoming connection |
| CONNECTION | Establish a connection with a waiting peer |
| RECEIVE | Block waiting for an incoming message |
| SEND | Sending a message to the peer |
| DISCONNECT | Terminate a connection |

**Connectionless Service Primitives**

There are 4 types of primitives for Connectionless Oriented Service:

|  |  |
| --- | --- |
| UNIDATA | This primitive sends a packet of data |
| FACILITY, REPORT | Primitive for enquiring about the performance of the network, like delivery statistics. |

## The Relationship of Services to Protocols

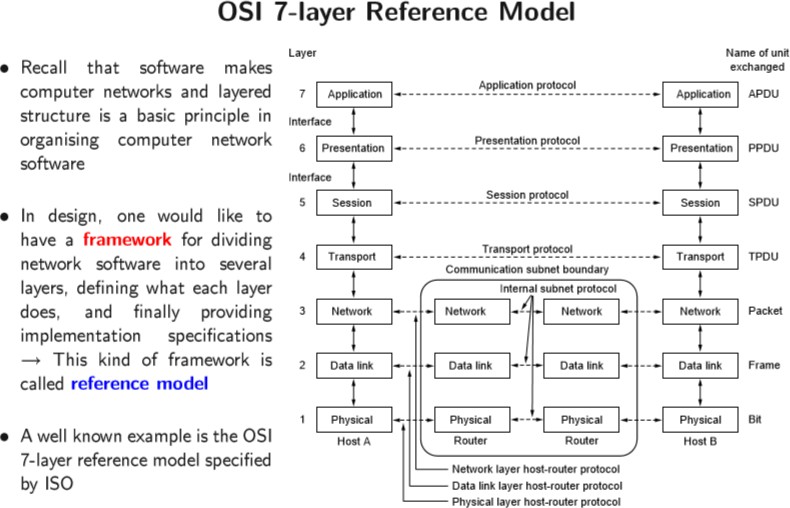
A service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

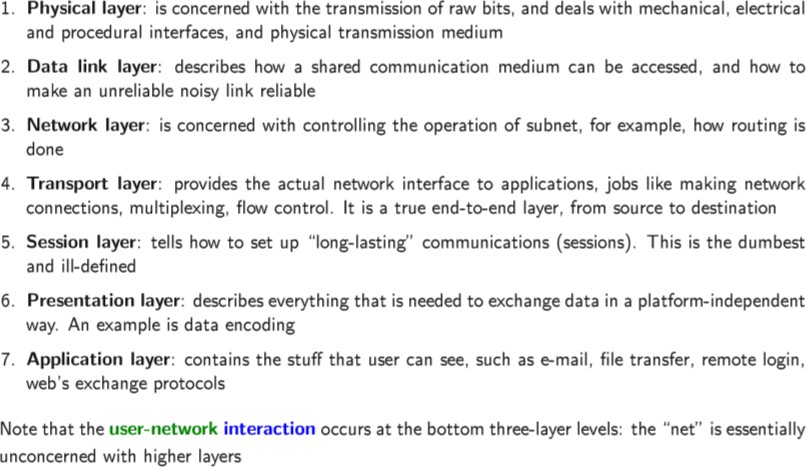
A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled.

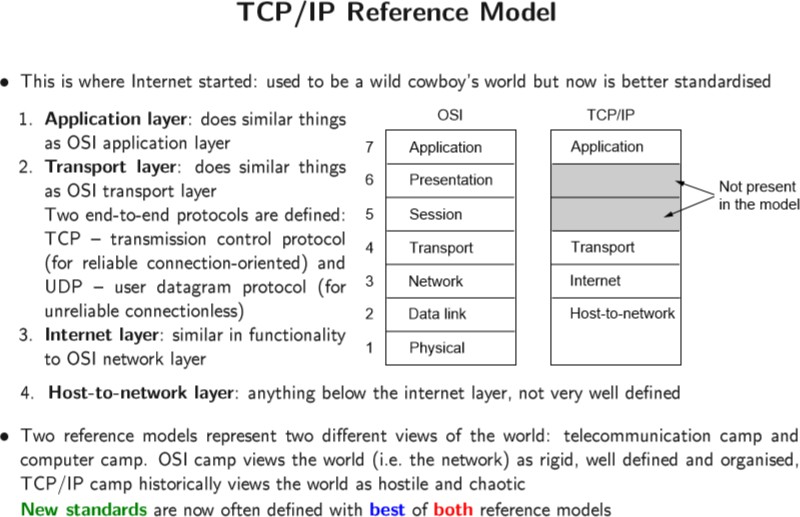
**1.1 Reference models (ISO-OSI, TCP/IP)**

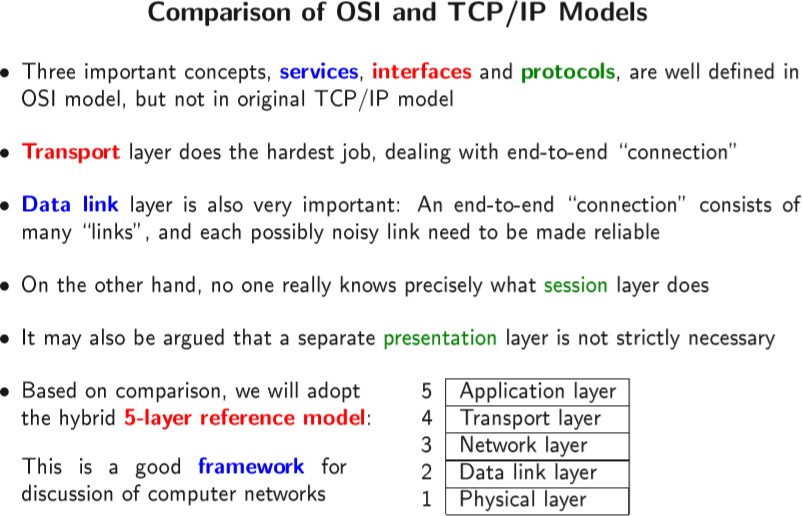
The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

* + 1. A layer should be created where a different abstraction is needed.
    2. Each layer should perform a well-defined function.
    3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
    4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
    5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy









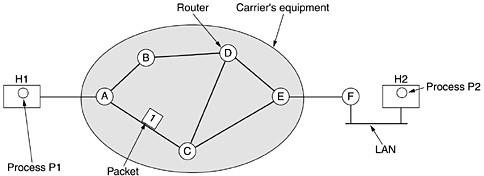
**1.2 Network Layer**

The network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination may require making many hops at intermediate routers along the way. To achieve its goals, the network layer must know about the topology of the communication subnet and choose appropriate paths through it. It must also take care to choose routes to avoid overloading some of the communication lines and routers while leaving others idle. Finally, when the source and destination are in different networks, new problems occur. It is up to the network layer to deal with them.

**1.2 Network Layer Design Issues**

The design issues include the service provided to the transport layer and the internal design of the subnet.

## Store-and-Forward Packet Switching



A host with a packet, transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

## Services Provided to the Transport Layer

The network layer provides services to the transport layer at the network layer/transport layer interface. The network layer services have been designed with the following goals in mind.

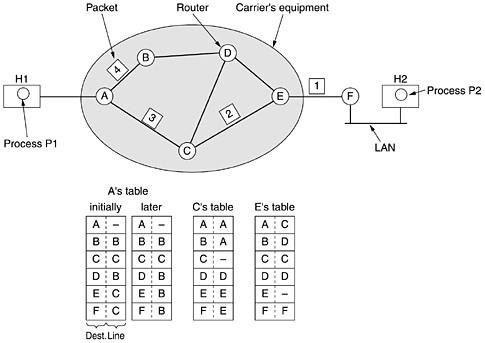
* 1. The services should be independent of the router technology.
  2. The transport layer should be shielded from the number, type, and topology of the routers present.
  3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Given these goals, the designers of the network layer have a lot of freedom in writing detailed specifications of the services to be offered to the transport layer.

## Implementation of Connectionless Service

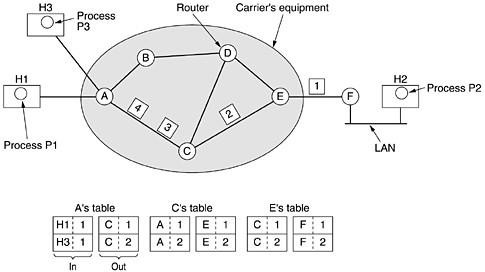
If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed. In this context, the packets are frequently called **datagrams** (in analogy with telegrams) and the subnet is called a **datagram subnet**. If connection-oriented service is used, a path from the source router to the destination router must be

established before any data packets can be sent. This connection is called a **VC** (**virtual circuit**), in analogy with the physical circuits set up by the telephone system, and the subnet is called a **virtual- circuit subnet**.



For connectionless service, for every packet a route must be selected and is not fixed. Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination. Only directly-connected lines can be used. The algorithm that manages the tables and makes the routing decisions is called the **routing algorithm**.

## Implementation of Connection-Oriented Service

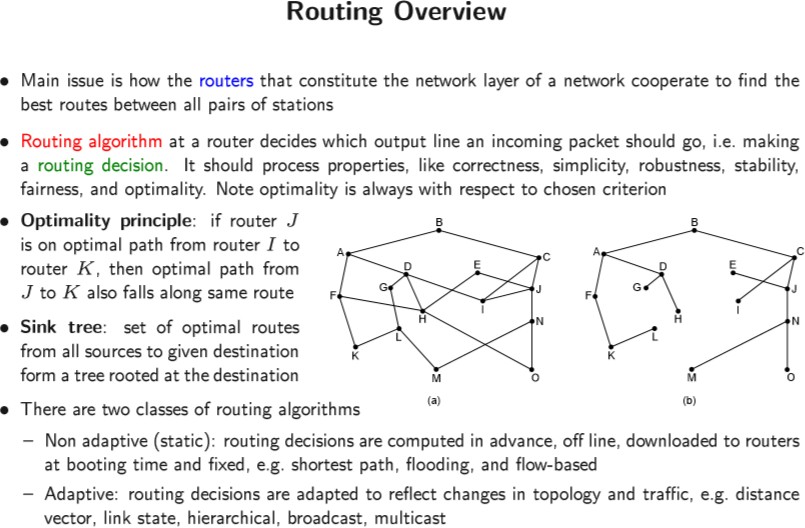
For connection-oriented service, we need a virtual-circuit subnet. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent, Instead, when a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the telephone system works. When the connection is released, the virtual circuit is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.

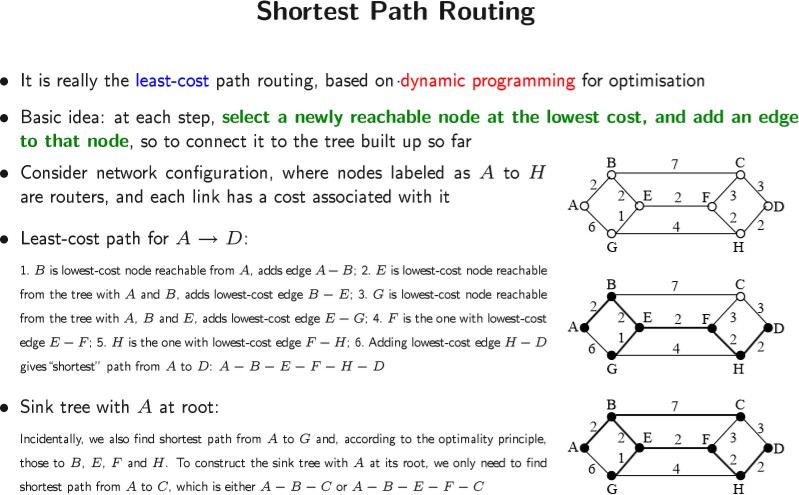
’

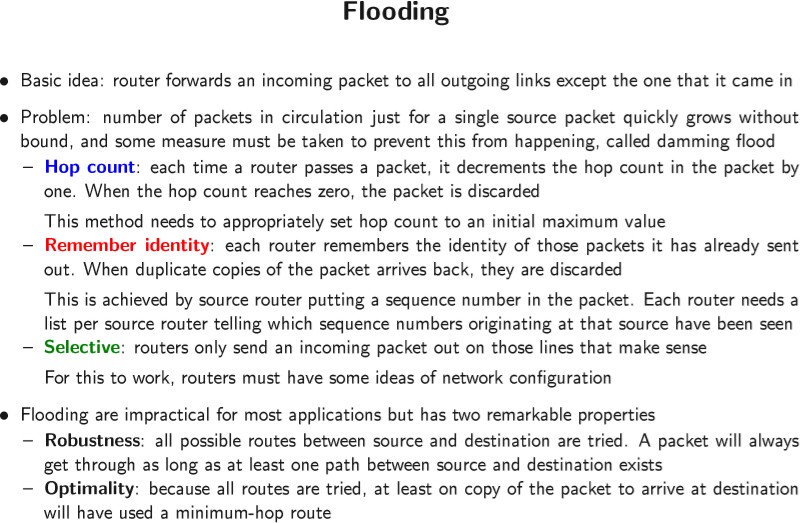
***Figure: Routing within a virtual-circuit subnet.***

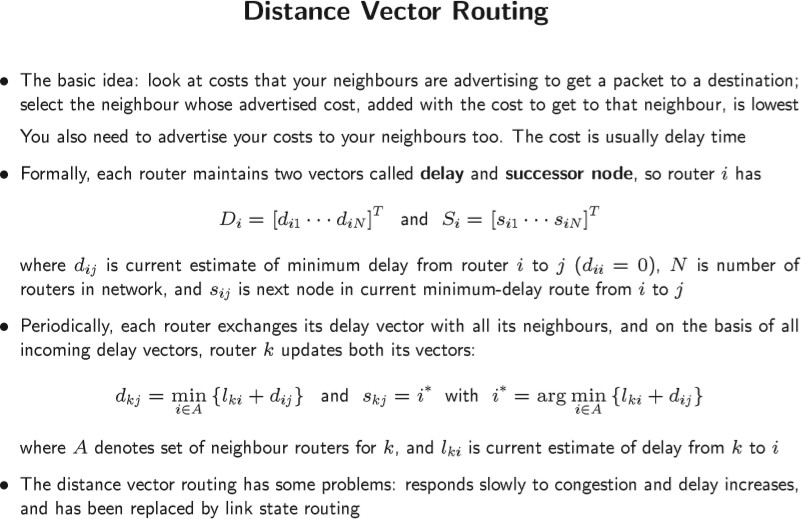
## Comparison of Virtual-Circuit and Datagram Subnets

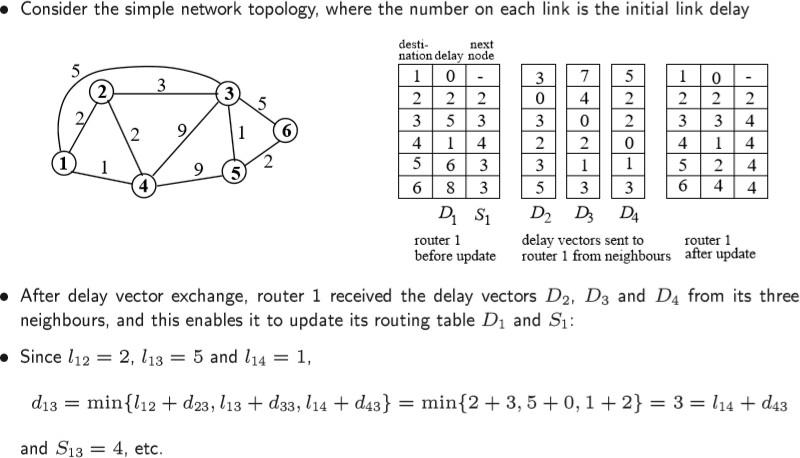
**1.2 Routing Algorithms**











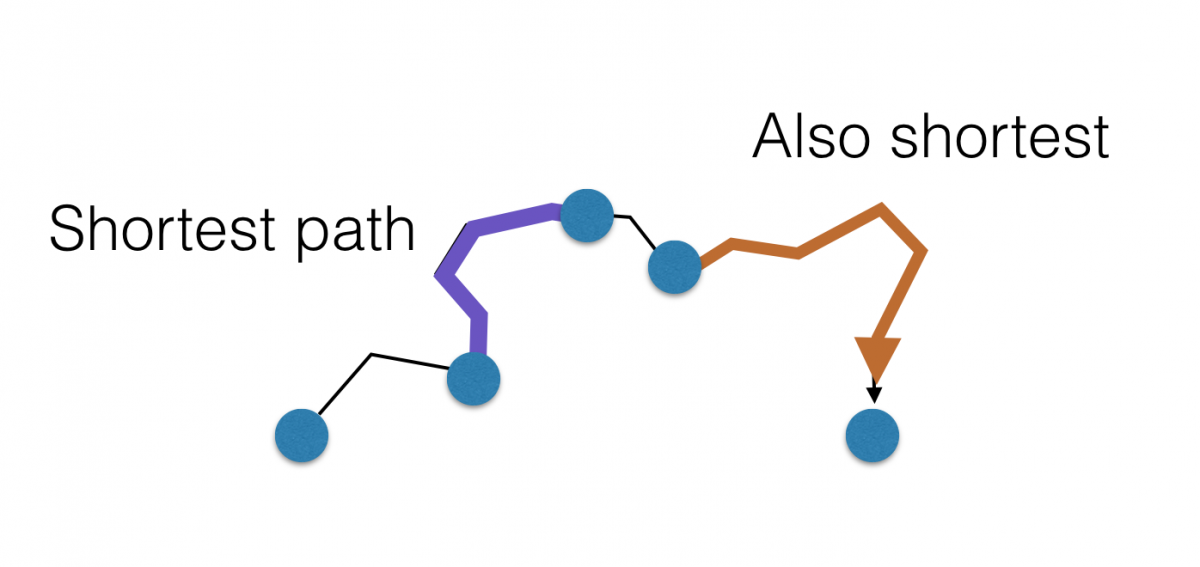
## link state / Dijkstra's Algorithm

**It algorithm allows us to find the shortest path between any two vertices of a graph.**

It differs from minimum spanning tree because the shortest distance between two vertices might not include all the vertices of the graph.

## How Dijkstra's Algorithm works

Dijkstra's Algorithm works on the basis that any subpath B -> D of the shortest path A -> D between vertices A and D is also the shortest path between vertices B and D.

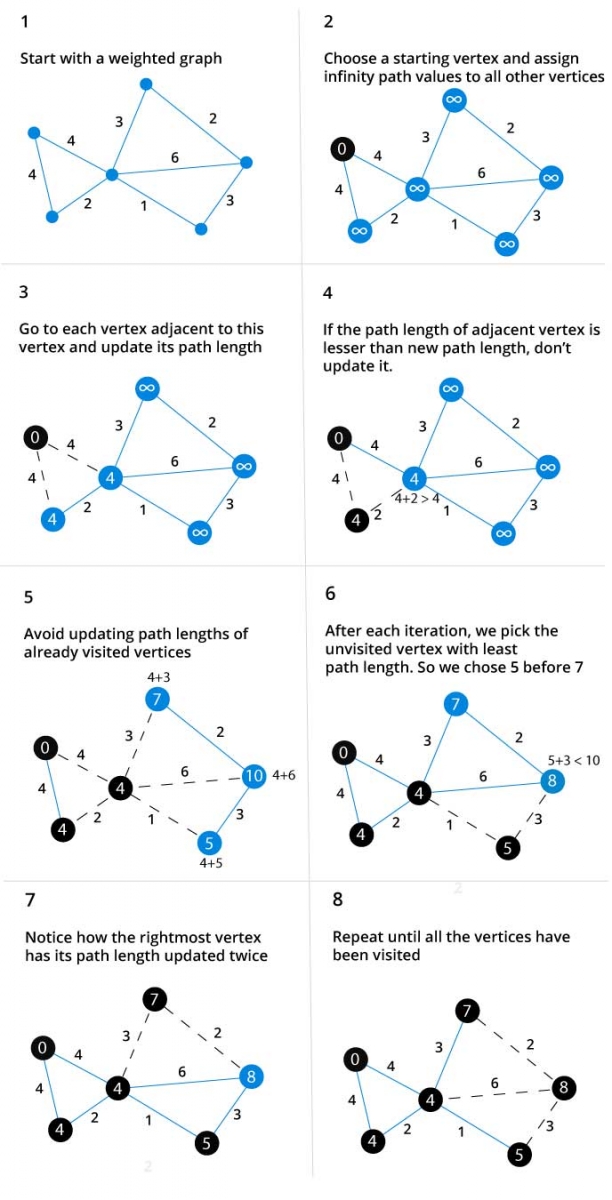


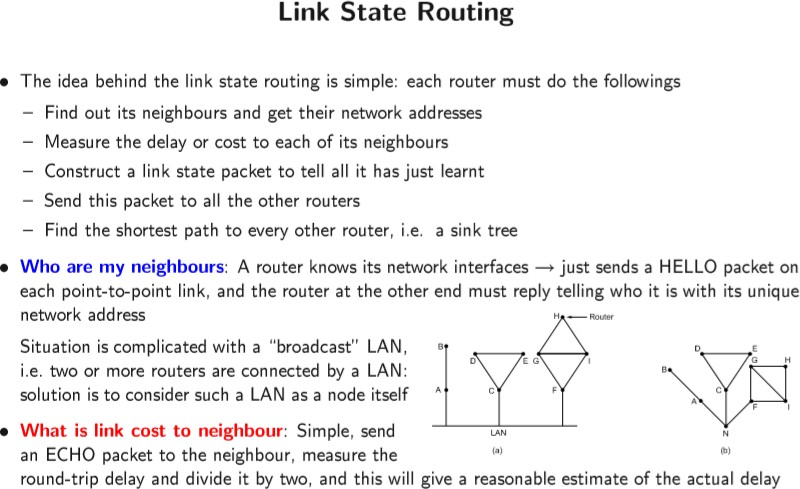
Djikstra used this property in the opposite direction i.e we overestimate the distance of each vertex from the starting vertex. Then we visit each node and its neighbours to find the shortest subpath to those neighbours.

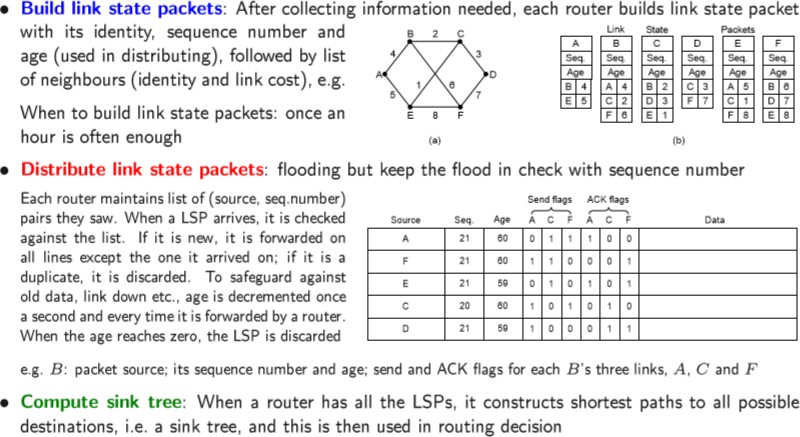
The algorithm uses a greedy approach in the sense that we find the next best solution hoping that the end result is the best solution for the whole problem.

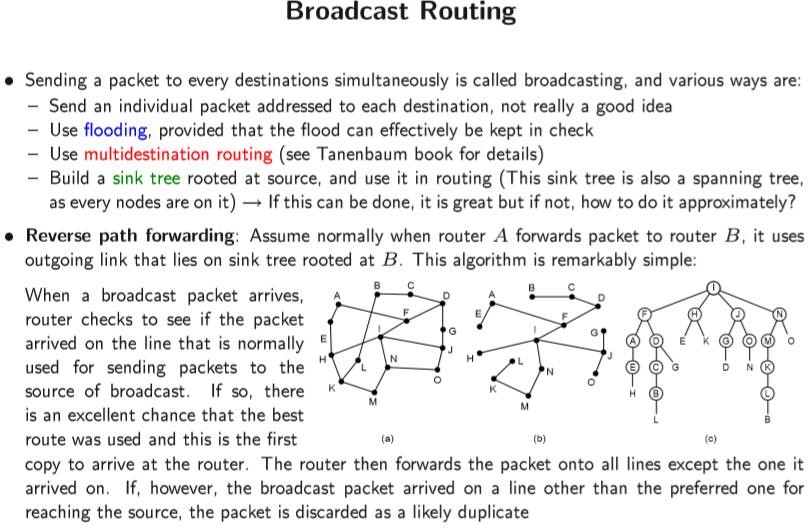
## Example of Dijkstra's algorithm

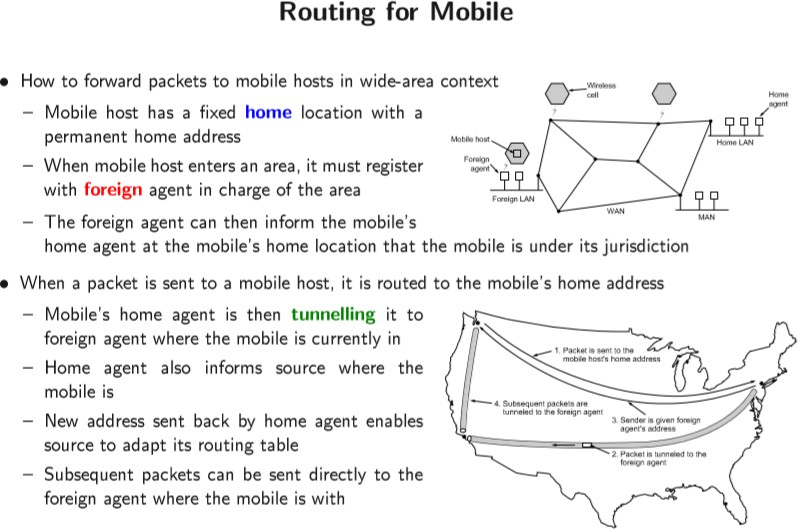
It is easier to start with an example and then think about the algorithm.

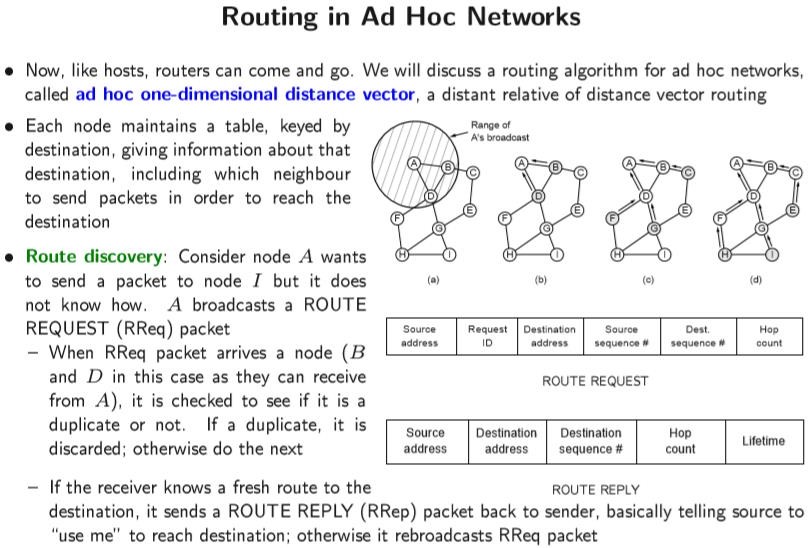


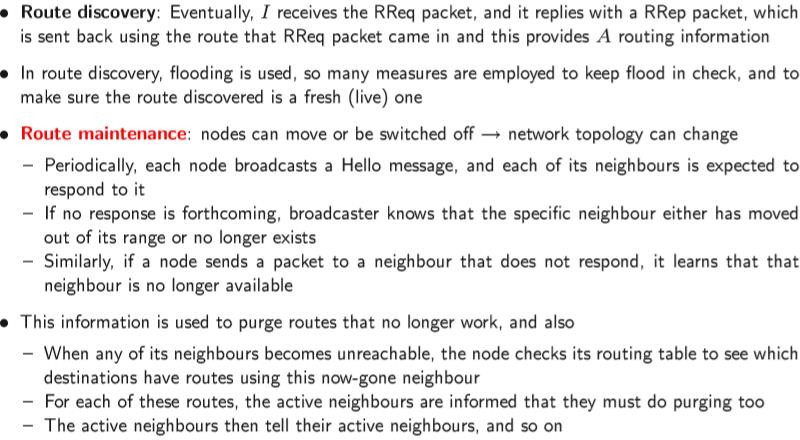




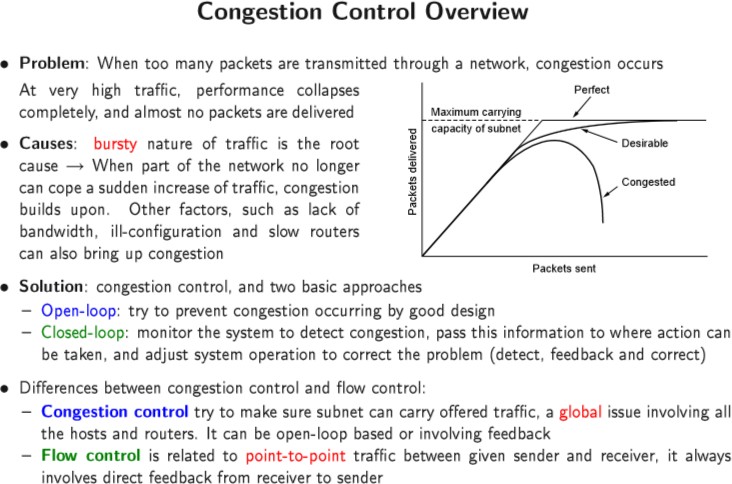


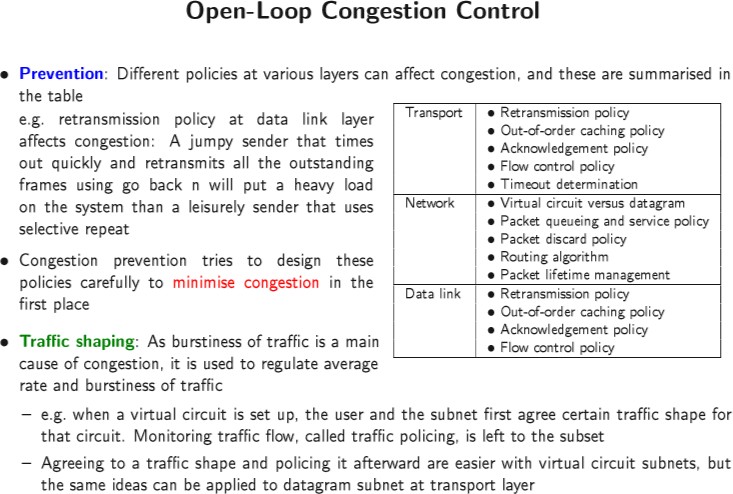


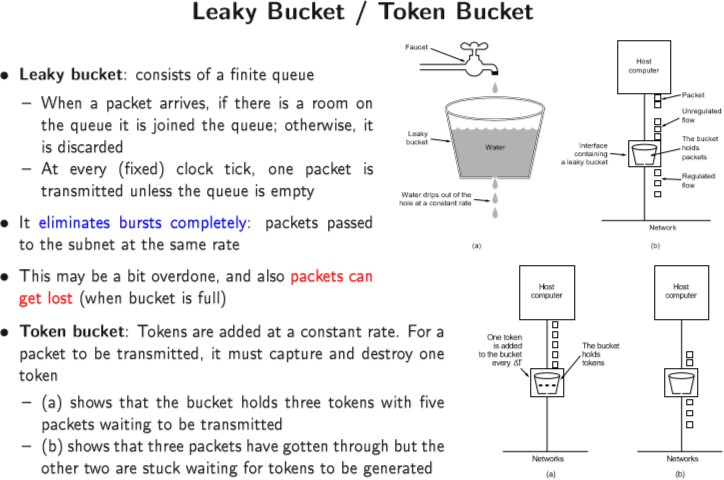


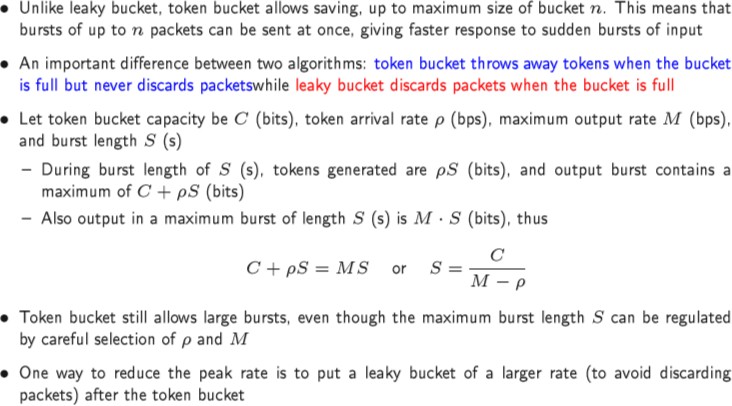


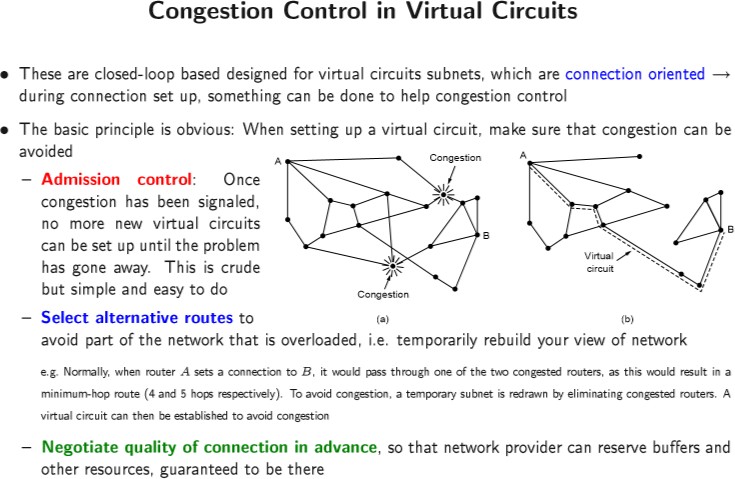
**1.2 Congestion Control Algorithms**

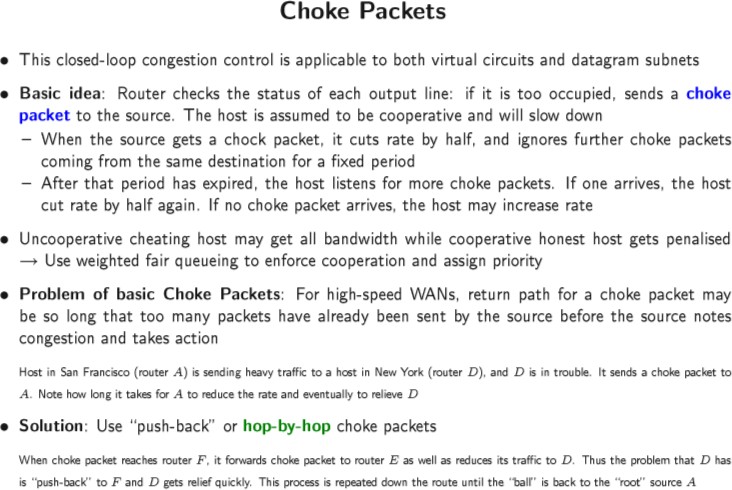












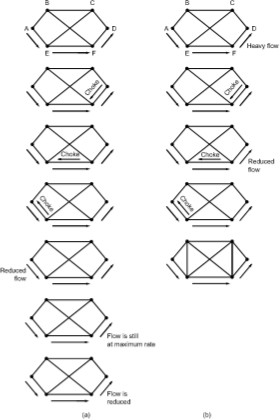


Figure: Choke packets in WANs: (a) basic, (b) hope-by-hope

