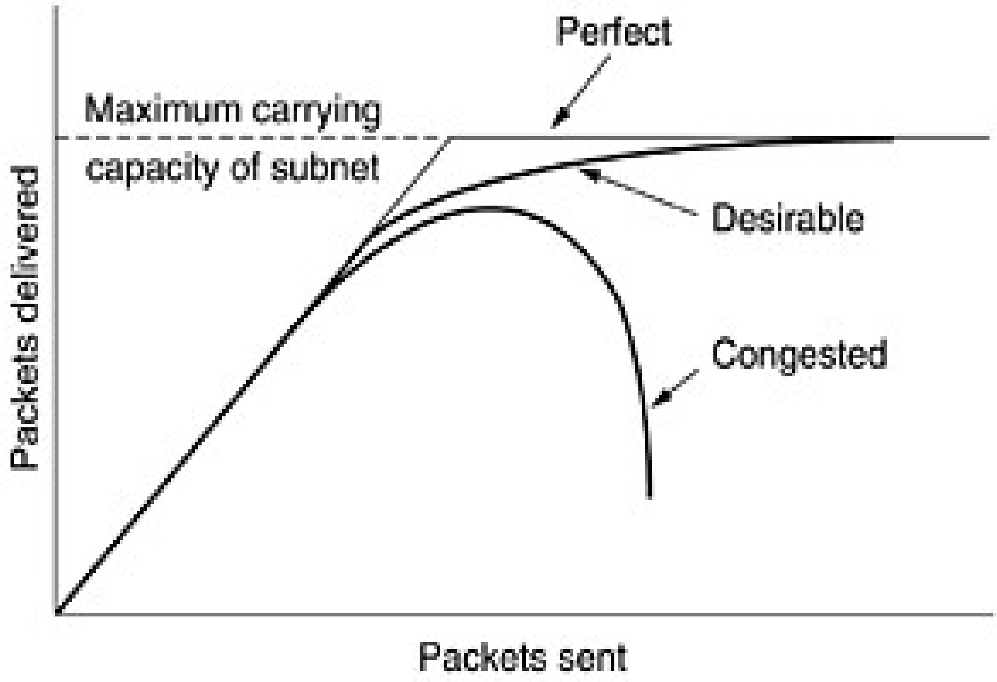
UNIT 3

Congestion Control Algorithms Internetworking and Quality of Service

Prof. Veena Gadad, Dept of CSE, RVCE,
Bangalore

Congestion

- When too many packets are present in (a part of) the subnet, performance degrades. This situation is called **congestion.**



- When the number of packets dumped into the subnet by the hosts is within its carrying capacity, they are all delivered.
- The number delivered is proportional to the number sent.
- As traffic increases too far, the routers are no longer able to cope and they begin losing packets.
- At very high trafffic, performance collapses completely and almost no packets are delivered.

Factors causing congestion

1. Streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up.
   - If there is insufficient memory to hold all of them, packets will be lost.
2. Slow processors in routers can also cause congestion.
3. Low-bandwidth lines can also cause congestion.
4. Any frequently mismatch between parts of the system may result in congestion and this problem will persist until all the components are in balance.

Congestion control vs Flow control

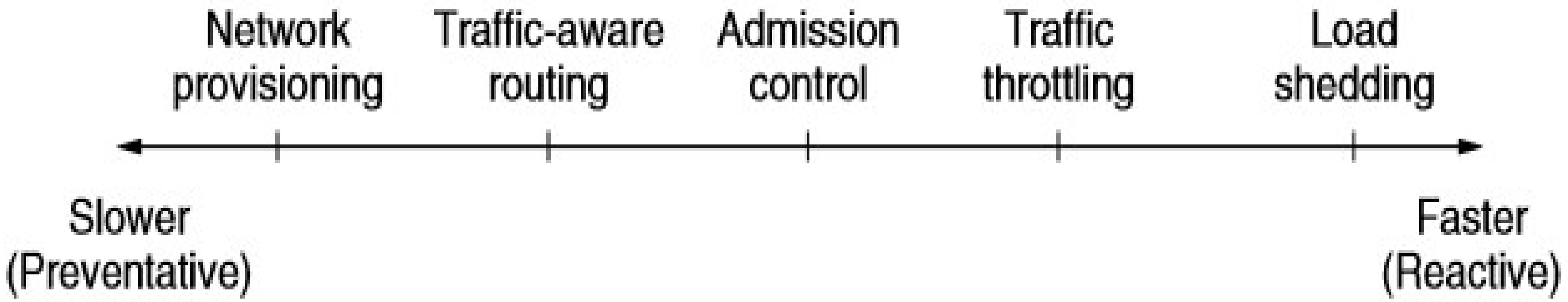
- **Congestion control** has to do with making sure the subnet is able to carry the offered traffic.
- It involves the behavior of all the hosts, all the routers, the store-and-forwarding processing within the routers, and all the other factors that tend to diminish the carrying capacity of the subnet.

- **Flow control**, in contrast, relates to the point-to-point traffic between a given sender and a given receiver.
- Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it.
- Flow control frequently involves some direct feedback from the receiver to the sender to tell the sender how things are doing at the other end.

- For example: consider a fiber optic network with a capacity of 1000 gigabits/sec on which a supercomputer is trying to transfer a file to a personal computer at 1 Gbps.
- There is no congestion (the network itself is not in trouble),
  - Flow control is needed to force the supercomputer to stop frequently to give the personal computer a chance to breathe.
- Consider a store-and-forward network with 1-Mbps lines and 1000 large computers, half of which are trying to transfer files at 100 kbps to the other half.
- The problem is not that of fast senders overpowering slow receivers, but that the total offered traffic exceeds what the network can handle.

Approaches to Congestion Control

- The presence of congestion means that the load is (temporarily) greater than the resources (in a part of the network) can handle.
- Two solutions: increase the resources or decrease the load.
- These solutions are usually applied on different time scales to either prevent congestion or react to it once it has occurred.



Timescales of approaches to congestion control.

Provisioning

- The most basic way to avoid congestion is to build a network that is well matched to the traffic that it carries.
- Resources can be added dynamically when there is serious congestion.
- More often, links and routers that are regularly heavily utilized are upgraded at the earliest opportunity.

Traffic Aware Routing

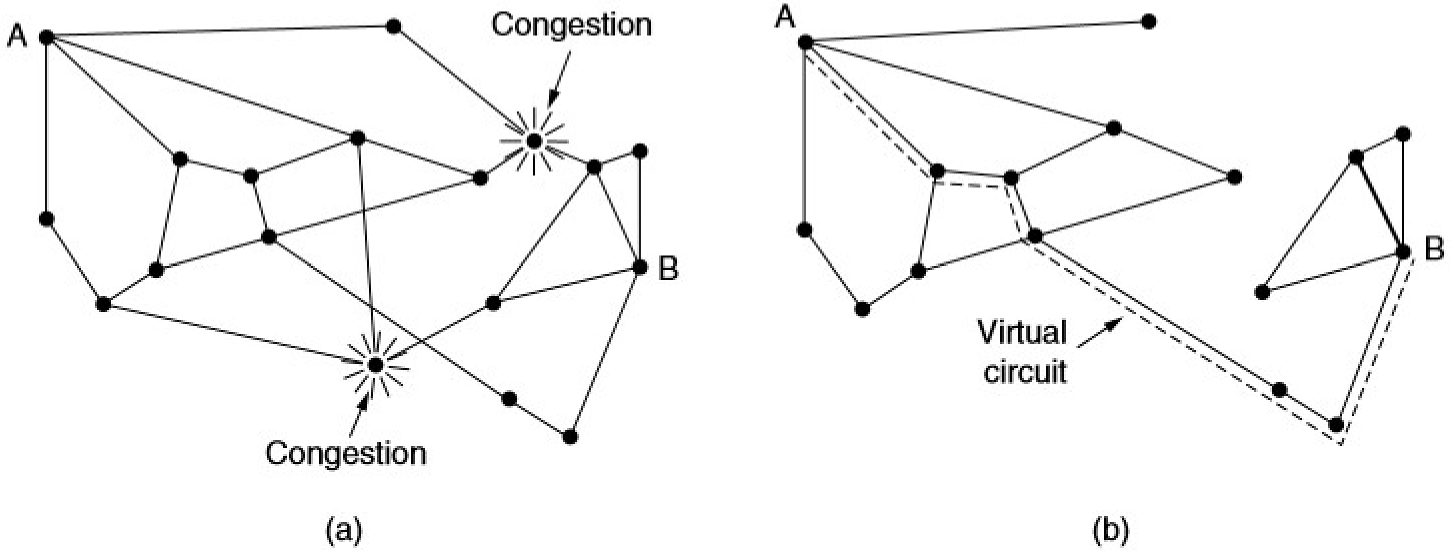
- To make the most of the existing network capacity, routes can be tailored to traffic patterns that change during the day as network users wake and sleep in different time zones.
- Splitting traffic across multiple paths is one of the solution.

Admission Control

- Sometimes it is not possible to increase capacity.
- The only way then to beat back the congestion is to decrease the load.
- In a virtual-circuit network, new connections can be refused if they would cause the network to become congested.
- Sending Feedback to the source to either slow down or to stop.

Admission Control and Traffic aware routing

- Admission control can also be combined with traffic-aware routing by considering routes around traffic hotspots as part of the setup procedure.



Traffic Throttling or Congestion Avoidance

- Senders adjust their transmissions to send as much traffic as the network can readily deliver.
- The network aims to operate just before the onset of congestion.
- When congestion is imminent, it must tell the senders to throttle back their transmissions and slow down- *Feedback*

- Traffic Throttling aims to solve two problems:
  1. Routers must determine when congestion is approaching, ideally before it has arrived.
     - Each router can continuously monitor the resources it is using.
       - The utilization of the output links.
       - Buffering of queued packets inside the router.
       - Number of packets that are lost due to insufficient buffering.
  2. Routers must deliver timely feedback to the senders that are causing the congestion.
     - Requires action on behalf of the senders that are using the network.
     - The router must identify the appropriate senders.

Queuing Delay

- To maintain a good estimate of the queueing delay, d, a sample of the instantaneous queue length, s, can be made periodically.
- d updated according to

  $d_{new} = \alpha\, d_{old} + (1 - \alpha)s$

  where the constant α determines how fast the router forgets recent history.

  – This is called an EWMA (Exponentially Weighted Moving Average).

Feedback mechanisms

1. Choke Packets

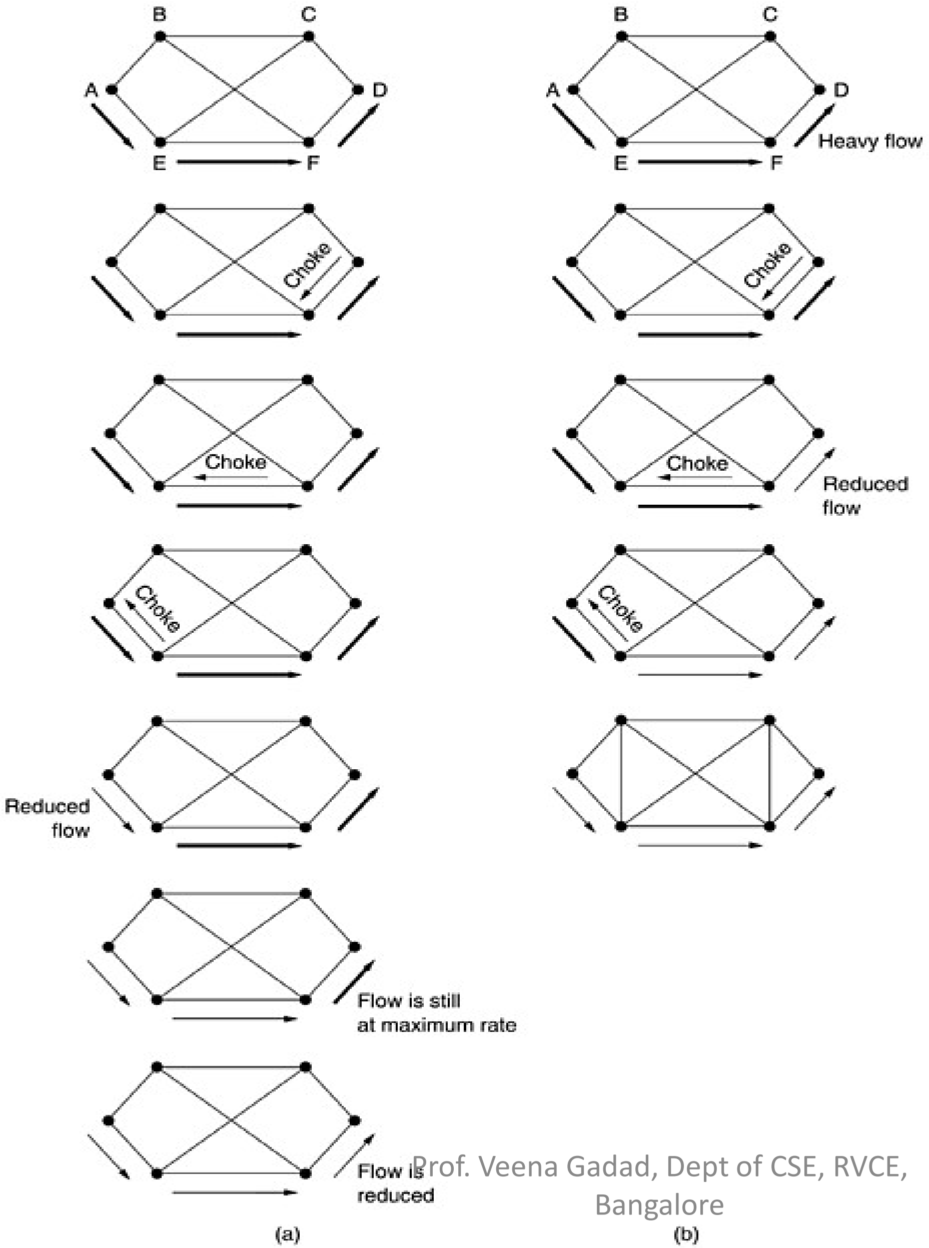
- Sending a warning bit is indirect way of telling the source to slow down.
- In this approach, the router sends a choke packet back to the source host.
- The original packet is tagged (a header bit is turned on) so that it will not generate any more choke packets farther along the path and is then forwarded in the usual way.
- When the source host gets the choke packet, it is required to reduce the traffic.
- After certain interval the host listens for choke packets, if received it slows down its transmission still more.

- Typically, the first choke packet causes the data rate to be reduced to 0.50 of its previous rate, the next one causes a reduction to 0.25, and so on.
- Increases are done in smaller increments to prevent congestion from reoccurring quickly.

2. Hop-by-hop choke packets

- At high speeds or over long distances, sending a choke packet to the source hosts does not work well because the reaction is so slow.
- An alternative approach is to have the choke packet take effect at every hop it passes through.
- The net effect of this hop-by-hop scheme is to provide quick relief at the point of congestion at the price of using up more buffers upstream.

Hop by hop choke packet.



3. Load shedding

- Load shedding action is taken when routers are being inundated by packets that they cannot handle, they just throw them away.
- A router can simply drop packets at random, but it could discard the packets depending on the applications running.
- For file transfer, **an old packet is worth** more than a new one, for multimedia, **a new packet** is more important than an old one.
- Intelligent discard policy- the packets must be marked as VERY IMPORTANT- NEVER, EVER DISCARD.
- The incentive might be in the form of money- **less pay- lower priority and packets are discarded.**

4. Random Early Detection (RED)

- It is always better to deal with congestion at the first point of detection.
- This observation leads to the idea of discarding packets before all the buffer space is really exhausted, the algorithm for doing this is RED.
- In some transport protocols (including TCP), the response to lost packets is for the source to slow down.
- TCP was designed for wired networks and wired networks are very reliable, so lost packets are mostly due to buffer overruns rather than transmission errors.
- By having routers drop packets before the situation has become hopeless the idea is that there is time for action to be taken before it is too late.

- To determine when to start discarding, routers maintain a running average of their queue lengths.
- When the average queue length on some line exceeds a threshold, the line is said to be congested and action is taken.
- The router usually picks the packet at random and discards it.
- The source will eventually notice the lack of acknowledgement and take action as it knows that lost packets are generally caused by congestion it responds by slowing down.
- In wireless networks, where most losses are due to noise on the air link, this approach cannot be used.

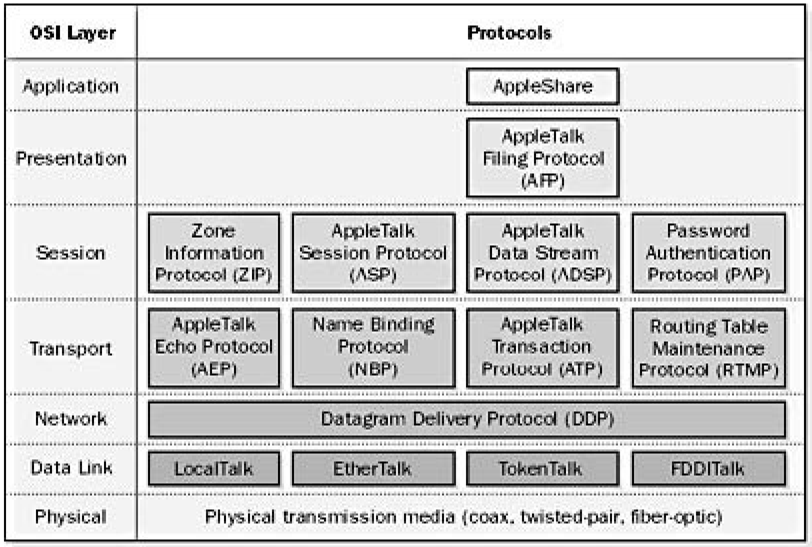
Internetworking

- Different networks exist, including LANs, MANs, and WANs.
- Numerous protocols are in widespread use in every layer.
- Internetworking is to connect two or more networks that are connected to form an internet.

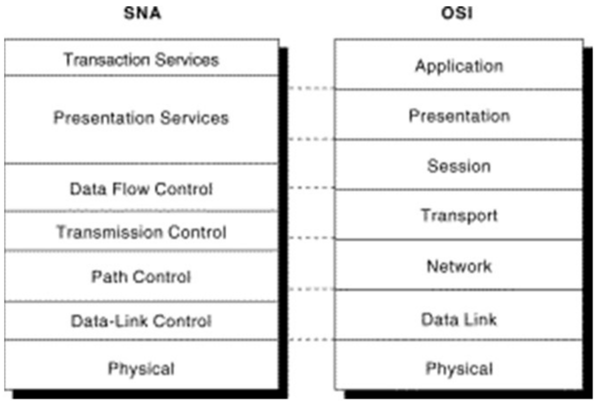
Why different networks and different protocols?

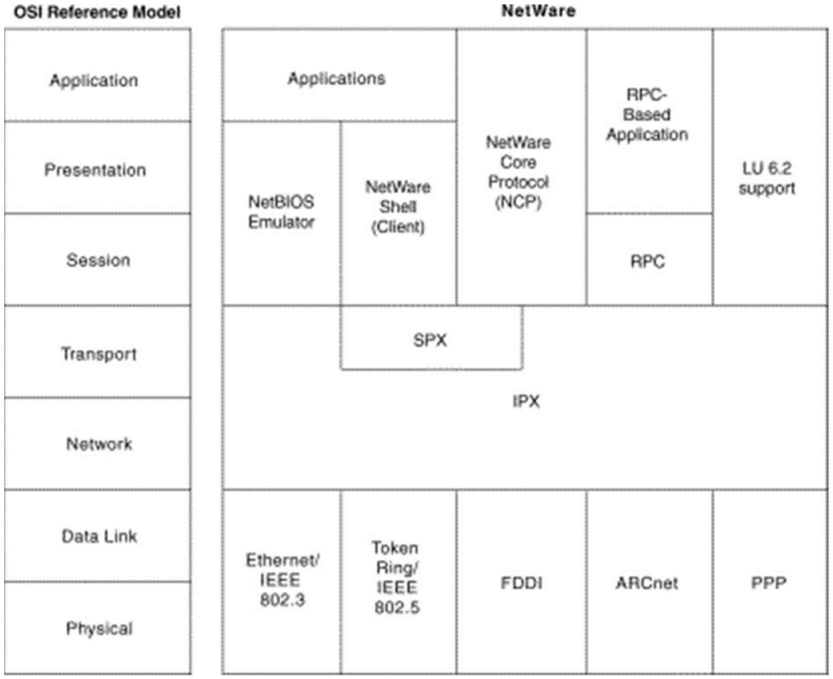
- First, the installed base of different networks is large – PC's run TCP/IP or Apple Talk or Novell NCP/IPX , Mainframes run IBM's SNA, Telephone systems use ATM Networks, Wireless use variety of different protocols.
- With new technology the protocols change.

- Second, Different OS- UNIX and running TCP/IP and some systems with Macs and Apple Talk.
- Third, different networks (e.g., ATM and wireless) have radically different technology hence different hardware.

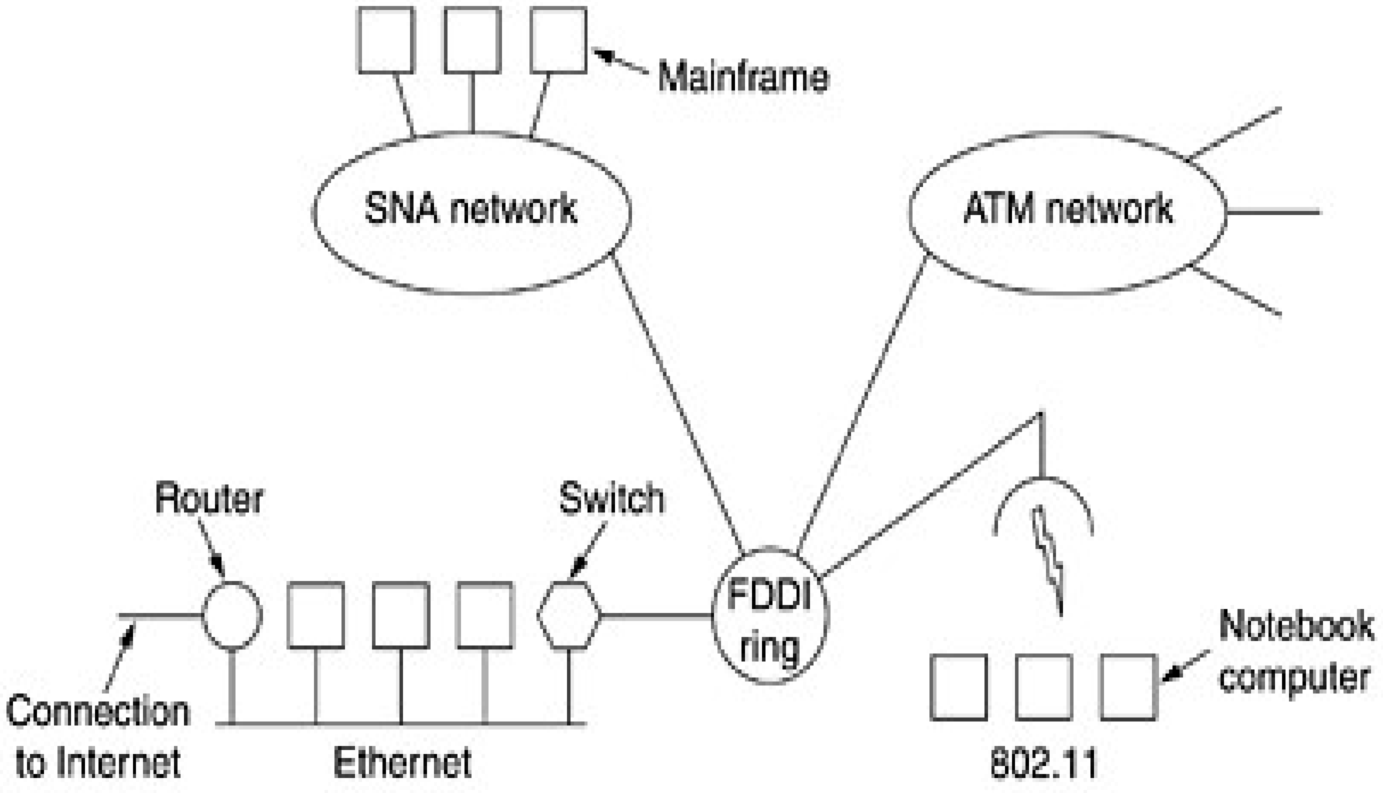


OSI Layer	Protocols			
Application			AppleShare	
Presentation			AppleTalk Filing Protocol (AFP)	
Session	Zone Information Protocol (ZIP)	AppleTalk Session Protocol (ASP)	AppleTalk Data Stream Protocol (ADSP)	Password Authentication Protocol (PAP)
Transport	AppleTalk Echo Protocol (AEP)	Name Binding Protocol (NBP)	AppleTalk Transaction Protocol (ATP)	Routing Table Maintenance Protocol (RTMP)
Network	Datagram Delivery Protocol (DDP)			
Data Link	LocalTalk	EtherTalk	TokenTalk	FDDITalk
Physical	Physical transmission media (coax, twisted-pair, fiber-optic)			





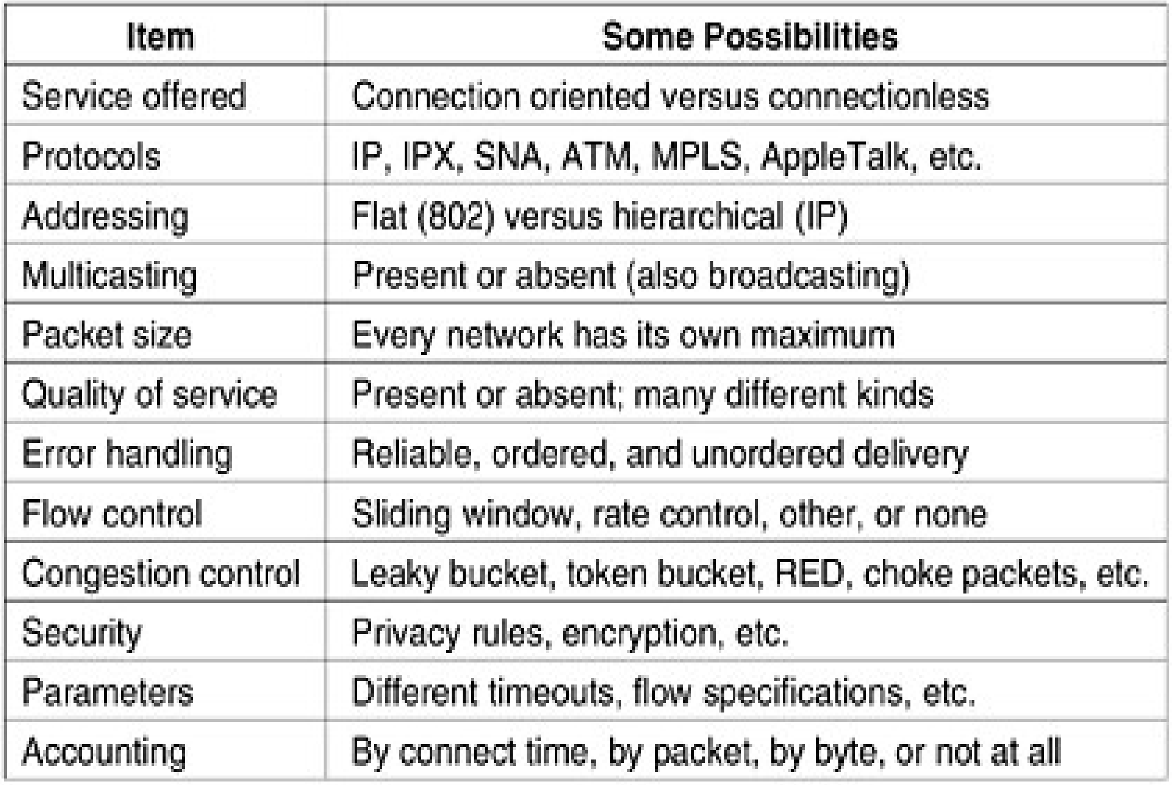
A collection of interconnected networks



- The purpose of interconnecting all these networks is to allow users on any of them to communicate with users on all the other ones and also to allow users on any of them to access data on any of them.
- Accomplishing this goal means sending packets from one network to another.
- Since networks often differ in important ways, getting packets from one network to another is not always so easy.

How Networks Differ?

- Networks can differ in many ways.
- Some of the differences, such as different modulation techniques or frame formats, are in the physical and data link layers.



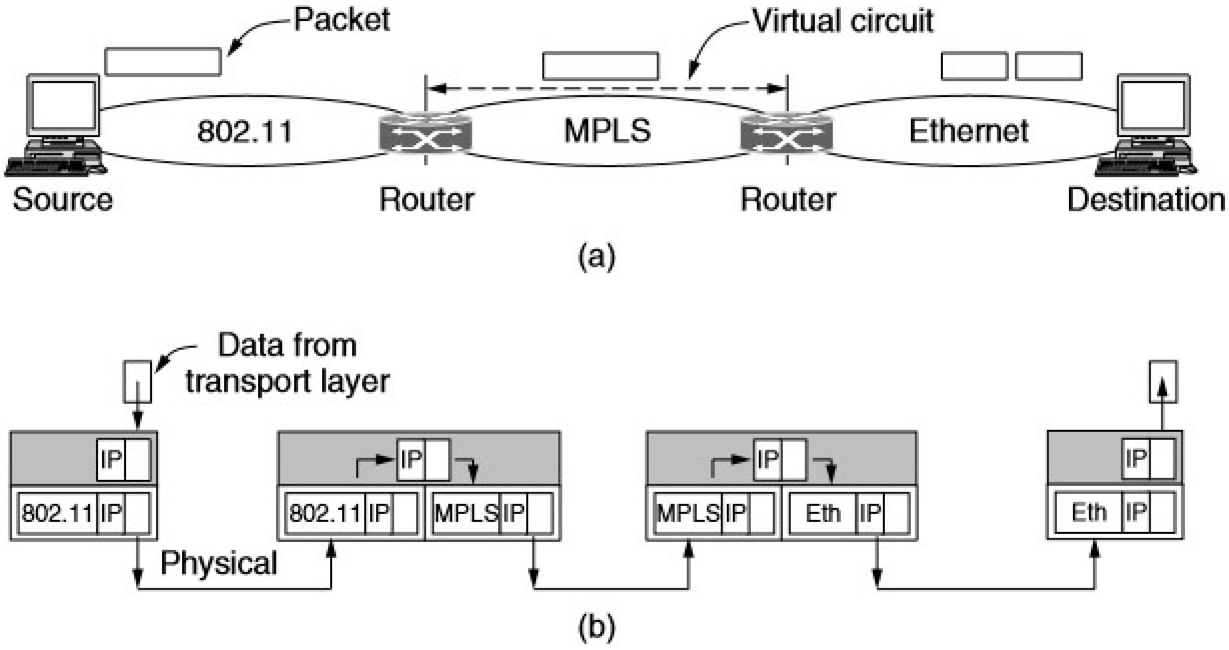
Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

How the networks can be connected?

- Networks can be interconnected by different devices.
- In the physical layer, networks can be connected by repeaters or hubs, which just move the bits from one network to an identical network.
- These are mostly analog devices and do not understand anything about digital protocols.
- At data link layer- bridges and switches
- They can accept frames, examine the MAC addresses, and forward the frames to a different network while doing minor protocol translation in the process
- For example, from Ethernet to FDDI or to 802.11.

Interconnection at higher layer

- An internet comprised of 802.11, MPLS, and Ethernet networks

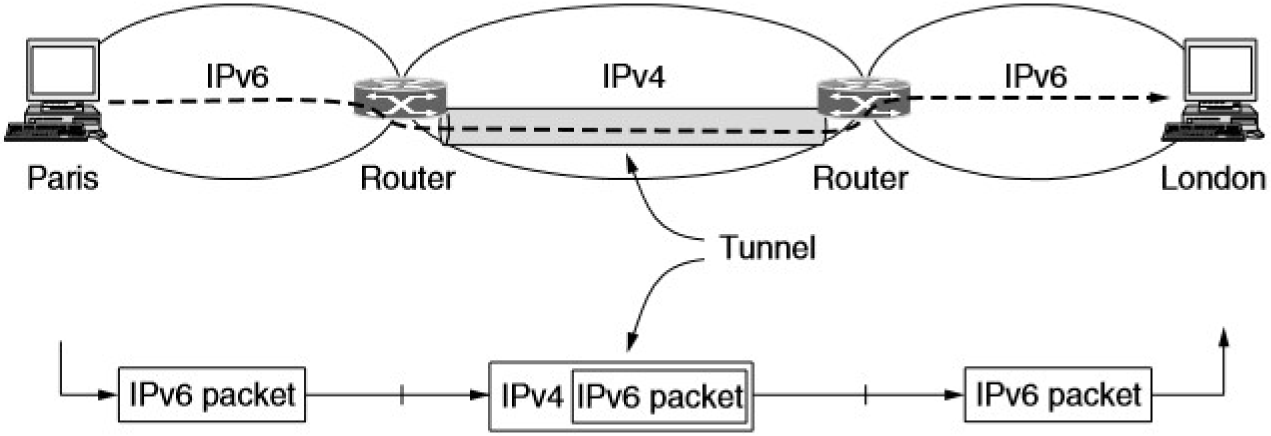


(a) A packet crossing different networks. (b) Network and link layer protocol processing.

- Different Networks- Different addressing format.
- 802.11 provides a connectionless service, but MPLS provides a connection-oriented service.
- This means that a virtual circuit must be set up to cross that network.
- If the packets are larger then must be broken down- Fragmentation and reassembled at destination.
- A router that can handle multiple network protocols is called a multiprotocol router.

Tunnelling

- Making two different networks interwork is exceedingly difficult.
- Special Case: the source and destination hosts are on the same type of network, but there is a different network in between.



- The path through the IPv4 Internet can be seen as a big tunnel extending from one multiprotocol router to the other.
- Tunneling is widely used to connect isolated hosts and networks using other networks.
- The network that results is called an **overlay** since it has effectively been overlaid on the base network.

Advantages:

1. Security: With tunnel we can create a private link across public network.
2. R1 and R2 may be multicast routers- some extra capabilities which are not available in other network.
3. To carry packets from protocols other than IP across an IP network.

Disadvantages

- Increases the length of packets; this might represent a significant waste of bandwidth for short packets.
- Longer packets might be subject to fragmentation, which has its own set of drawbacks.
- There may also be performance implications for the routers at either end of the tunnel.
- There is a management cost for the administrative entity.

Internetwork Routing

- Different network- Different routing algorithms.
- Networks run by different operators lead to bigger problems.
- The operators may have different ideas about what is a good path through the network.
- This will lead the operators to use different quantities to set the shortest-path costs (e.g., milliseconds of delay vs. monetary cost).
- Shortest paths on the internet will not be well defined.

- Two level routing algorithms-
  - Intra domain or interior gateway routing
  - Inter domain or exterior gateway routing.
- Usually there will be different intra domain routing but same inter domain protocol.
- In the Internet, the interdomain routing protocol is called BGP (Border Gateway Protocol).

Autonomous systems and Routing Policies.

- A network that operates independently is called as an Autonomous system- e.g- ISP.
- An ISP network may be comprised of more than one AS .
- There are business arrangements between ISPs
  - Each ISP may charge or receive money from the other ISPs for carrying traffic.
  - Routing that requires crossing international boundaries- must take care of privacy laws.

Fragmentation

Each network imposes some maximum size on its packets. These limits have various causes, among them:

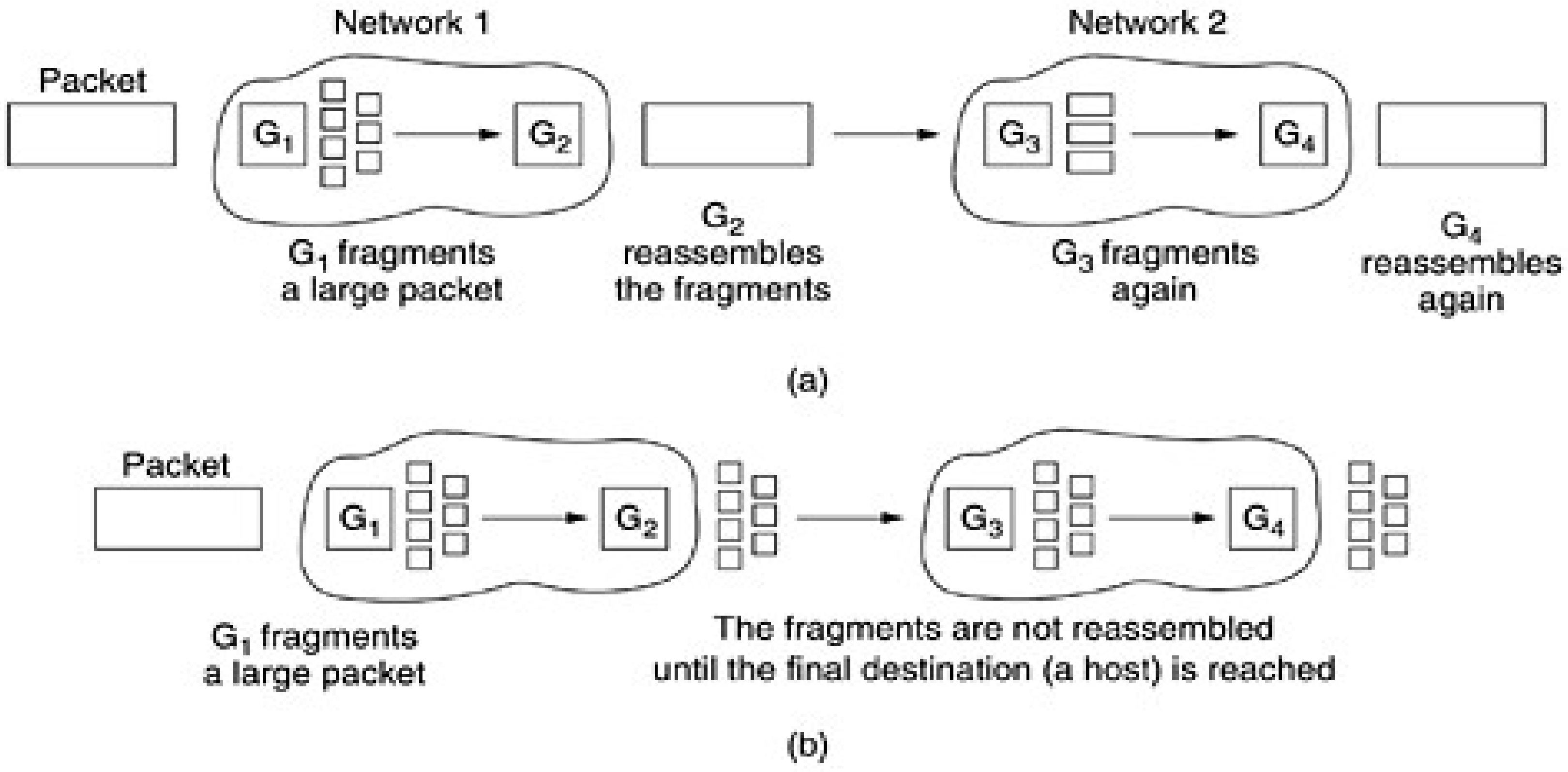
1. Hardware (e.g., the size of an Ethernet frame).
2. Operating system (e.g., all buffers are 512 bytes).
3. Protocols (e.g., the number of bits in the packet length field).
4. Compliance with some (inter)national standard.
5. Desire to reduce error-induced retransmissions to some level.
6. Desire to prevent one packet from occupying the channel too long.

- The result of all these factors is that the network designers are not free to choose any maximum packet size they wish.
- Maximum payloads range from 48 bytes (ATM cells) to 65,515 bytes (IP packets), although the payload size in higher layers is often larger.
- An obvious problem appears when a large packet wants to travel through a network whose maximum packet size is too small.
- The obvious solution is to allow gateways to break up packets into fragments, sending each fragment as a separate internet packet.

There are two types of fragmentations

a) Transparent Fragmentation

b) Non transparent fragmentation


Network 1
Network 2
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
G_2 reassembles the fragments
G_3 fragments again
G_4 reassembles again
(a)
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
The fragments are not reassembled until the final destination (a host) is reached
(b)

a) Transparent Fragmentation

- In this approach, the small-packet network has gateways (most likely, specialized routers) that interface to other networks.
- When an oversized packet arrives at a gateway, the gateway breaks it up into fragments.
- Each fragment is addressed to the same exit gateway, where the pieces are recombined.
- In this way passage through the small-packet network has been made transparent.
- Subsequent networks are not even aware that fragmentation has occurred.
- ATM networks, for example, have special hardware to provide transparent fragmentation of packets into cells and then reassembly of cells into packets.
- In the ATM world, fragmentation is called segmentation;

D’tages

- The exit gateway must know when it has received all the pieces, so either a count field or an "end of packet" bit must be provided.
- All packets must exit via the same gateway.
- Overhead required to repeatedly reassemble and then refragment a large packet passing through a series of small-packet networks.

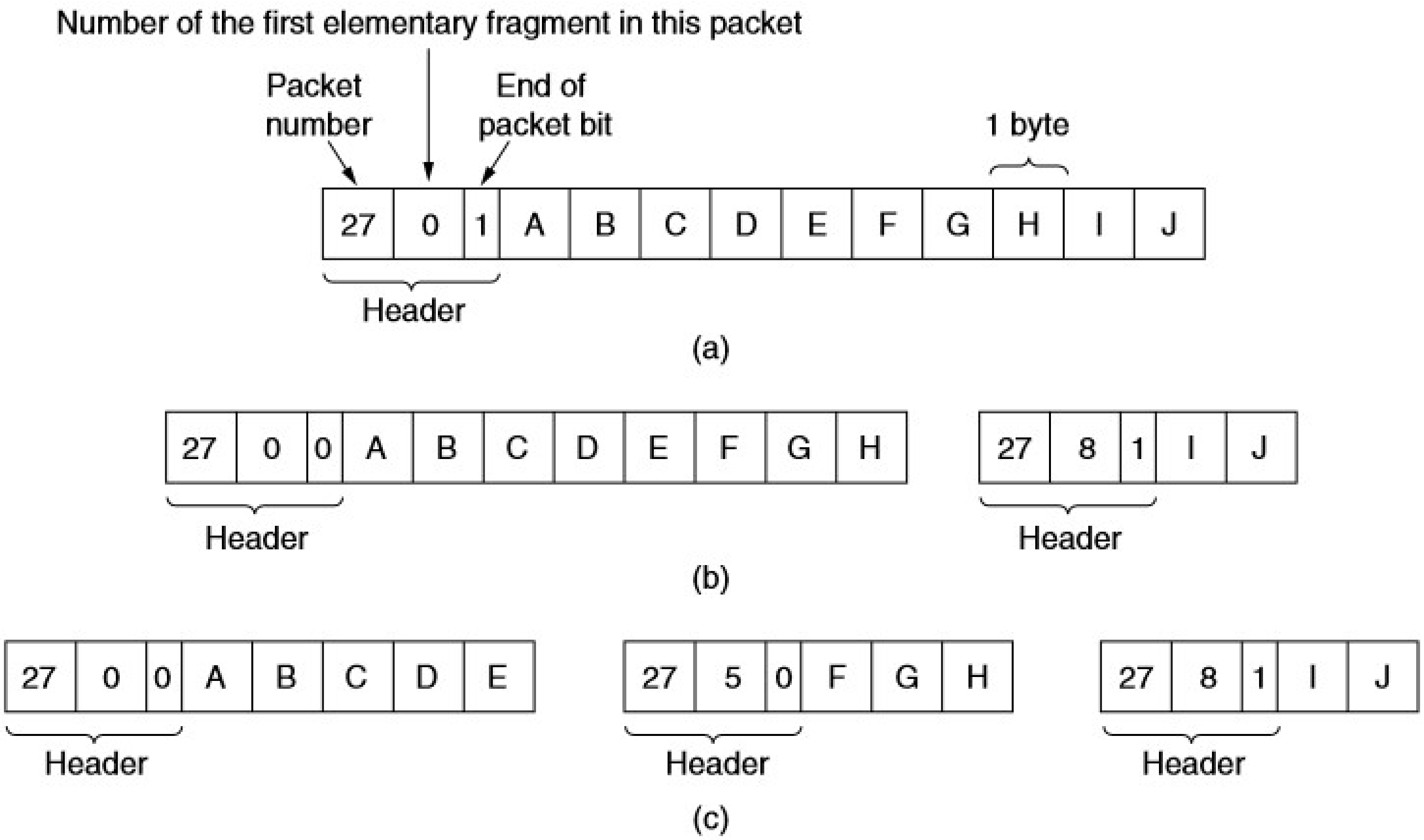
❖ATM requires transparent fragmentation.

a) Non transparent fragmentation

- In this approach the recombining of fragments does not occur at intermediate gateways.
- Once a packet has been fragmented, each fragment is treated as though it were an original packet.
- All fragments are passed through the exit gateway.
- Recombination occurs only at the destination host.

❖ Example of non transparent fragmentation is IP network.

- A complete design requires that the fragments be numbered in such a way that the original data stream can be reconstructed.
  - The design used by IP is to give every fragment a packet number (carried on all packets).
  - An absolute byte offset within the packet.
  - A flag indicating whether it is the end of the packet.


Number of the first elementary fragment in this packet
Packet number
End of packet bit
1 byte
27 0 1 A B C D E F G H I J
Header
(a)
27 0 0 A B C D E F G H
Header
27 8 1 I J
Header
(b)
27 0 0 A B C D E
Header
27 5 0 F G H
Header
27 8 1 I J
Header
(c)

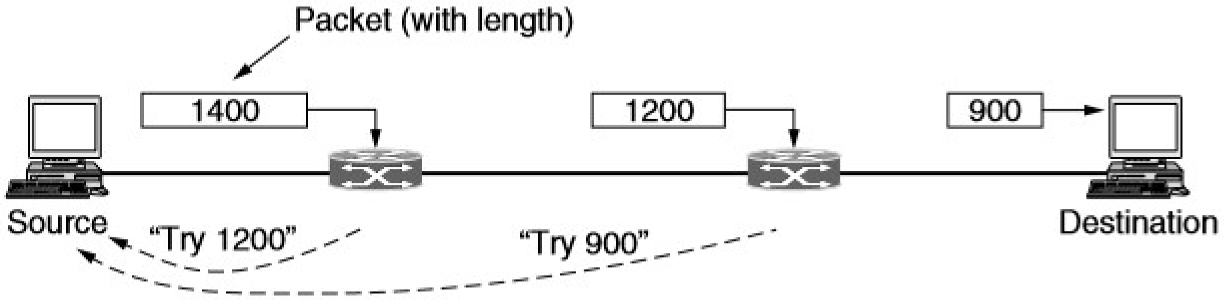
D’tages

- It requires *every host to be able to do reassembly.*
- When a large packet is fragmented, the total overhead increases because each fragment must have a header.

IPV6 and Fragmentation

- Modern Internet gets rid of the fragmentation.
- Uses the process is called path MTU discovery.
- Each IP packet is sent with its header bits set to indicate that no fragmentation is allowed to be performed.
- If a router receives a packet that is too large, it generates an error packet, returns it to the source, and drops the packet.

- When the source receives the error packet, it uses the information inside to refragment the packet into pieces that are small enough for the router to handle.
- If a router further down the path has an even smaller MTU, the process is repeated.



Advantages:

1. Source knows the packet length to be transmitted.
2. If the routes and path MTU change, new error packets will be triggered and the source will adapt to the new path.

Disadvantages:

1. Added startup delays simply to send a packet.
2. Source needs to find the MTU before transmission.

Quality of service

- Some applications (and customers) that demand stronger performance guarantees from the network than ‘‘the best that could be done under the circumstances.’’
- An easy solution to provide good quality of service is to build a network with enough capacity for whatever traffic will be thrown at it- Over Provisioning.

- Over Provisioning is expensive.
- Quality of service mechanisms let a network with less capacity meet application requirements at well at a lower cost.
- Four issues must be addressed to ensure quality of service:

1. What applications need from the network.
2. How to regulate the traffic that enters the network.
3. How to reserve resources at routers to guarantee performance.
4. Whether the network can safely accept more traffic.

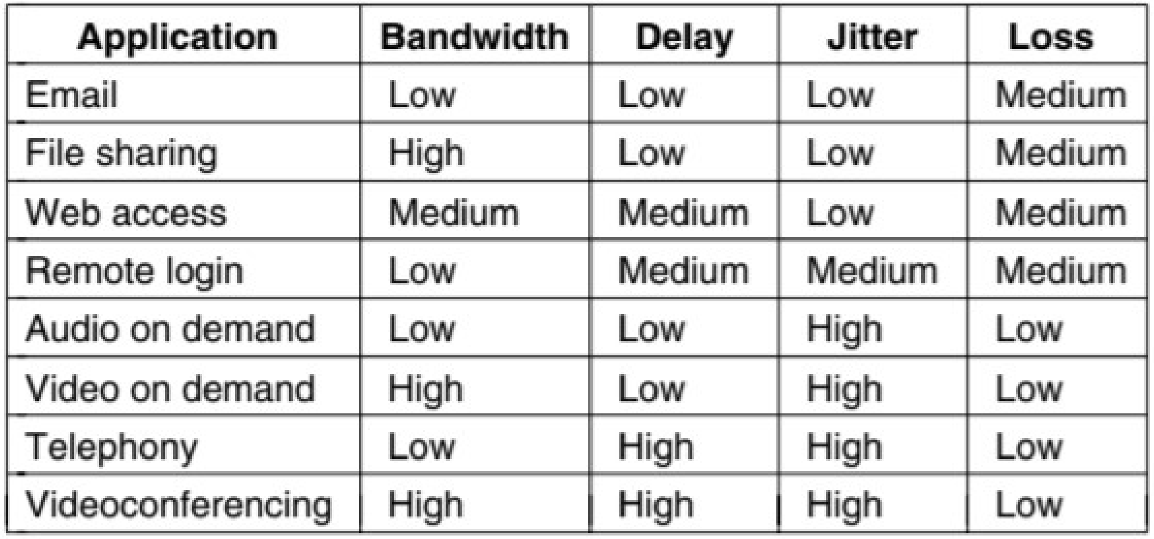
- No single technique deals efficiently with all these issues.
- A variety of techniques have been developed for use at the network (and transport) layer.
- Practical quality-of-service solutions combine multiple techniques.
- There are two versions of quality of service for the Internet called Integrated Services and Differentiated Services.

Application Requirement

- A stream of packets from a source to a destination is called a **flow.**
- A flow might be all the packets of a connection in a connection-oriented network, or all the packets sent from one process to another process in a connectionless network.
- The needs of each flow is characterized by four primary parameters: bandwidth, delay, jitter, and loss.
- These determine the QoS (Quality of Service) the flow requires.

- *Bandwidth*- the amount of data that can be sent from one point to another in a certain period of time.
- *Delay*- specifies how long it takes for a bit of data to travel across the **network** from one communication endpoint to another.
- *Jitter* - the variation in latency — the delay between when a signal is transmitted and when it is received.
- *Loss*- Failure of packets to reach destination, caused by error in transmission or due to congestion.

Stringency of applications' quality-of-service requirements



Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio on demand	Low	Low	High	Low
Video on demand	High	Low	High	Low
Telephony	Low	High	High	Low
Videoconferencing	High	High	High	Low

Traffic Shaping

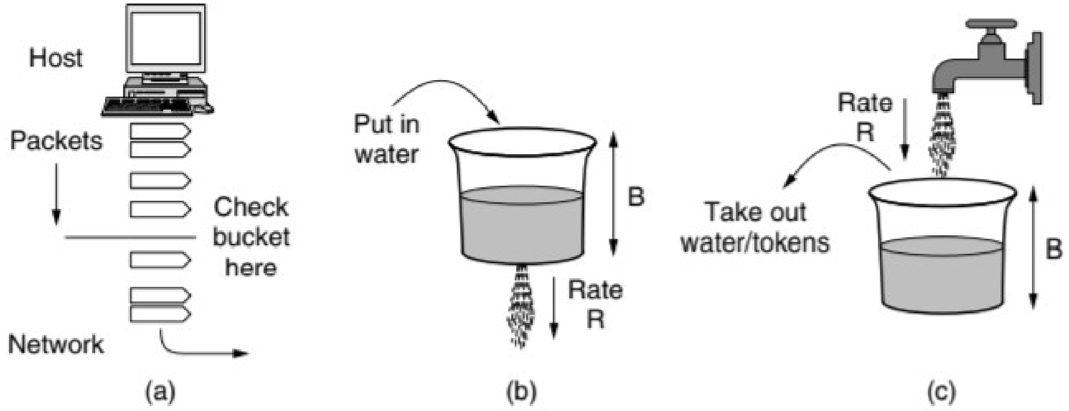
- Traffic in data networks is bursty.
- It typically arrives at nonuniform rates as the traffic rate varies- User interact with applications and computer switch between the tasks.
- Bursts of traffic are more difficult to handle than constant-rate traffic because they can fill buffers and cause packets to be lost.

- Traffic shaping is a technique for regulating the average rate and burstiness of a flow of data that enters the network.
- When a flow is set up, the user and the network (i.e., the customer and the provider) agree on a certain traffic pattern (i.e., shape) for that flow- Service Level Aggrement.
- Traffic shaping reduces congestion and thus helps the network live up to its promise.
- Packets in excess of the agreed pattern might be dropped by the network, or they might be marked as having lower priority.
- Monitoring a traffic flow is called traffic policing.

Leaky bucket and Token bucket algorithms

- These algorithms are used to characterize the traffic and monitor the data rate.

Leaky bucket and token bucket concept



. (a) Shaping packets. (b) A leaky bucket. (c) A token bucket.

Leaky Bucket Algorithm

- Each host is connected to the network by an interface containing a leaky bucket.
- To send a packet into the network, it must be possible to put more water into the bucket.
- If a packet arrives when the bucket is full, the packet must either be queued until enough water leaks out to hold it or be discarded.
- The former might happen at a host shaping its traffic for the network as part of the operating system.
- The latter might happen in hardware at a provider network interface that is policing traffic entering the network

Leaky Bucket Algorithm

- Step - 1 : Initialize the counter to **‘n’** at every tick of clock.
- Step - 2 : If **n** is greater than the size of packet in the front of queue send the packet into the network and decrement the counter by size of packet. Repeat the step until **n** is less than the size of packet.
- Step - 3 : Reset the counter and go to Step - 1.

Example

Let **n** = 1000

Packet =.

200	700	500	450	400	200

Since n > front of Queue i.e. n>200
Therefore, n= 1000-200 = 800
Packet size of 200 is sent to the network

200	700	500	450	400

Now Again n > front of queue i.e. n > 400
Therefore, n= 800-400 = 400
Packet size of 400 is sent to the network

200	700	500	450

Since n < front of queue .
There fore, the procedure is stop.

And we initialize **n = 1000** on another tick of clock.

This procedure is repeated until all the packets is sent to the network.

Token bucket algorithm

- The network interface as a bucket that is being filled.
- The tap is running at rate R and the bucket has a capacity of B.
- To send a packet, take out water (called tokens) from the bucket.
- No more than a fixed number of tokens, B, can accumulate in the bucket.
- If the bucket is empty wait until more tokens arrive before another packet can be sent.

Token Bucket Algorithm

Algorithm

Step - 1 : A token is added at every Δt time.

Step - 2 : The bucket can hold at most **b-**tokens. If a token arrive when bucket is full it is discarded.

Step - 3 : When a packet of **m** bytes arrived **m** tokens are removed from the bucket and the packet is sent to the network.

Step – 4 : If less than **m** tokens are available no tokens are removed from the buckets and the packet is considered to be **non conformant**.
The **non conformant** packet may be enqueued for subsequent transmission when sufficient token have been accumulated in the bucket.

If **B** is the maximum capacity of bucket and **R** is the arrival rate and **M** is the maximum output rate then Burst Length **S** can be calculated as

$$\boxed{B + RS = MS}$$

This equates to

$S=B/(M-R)$

Example: B=250KB, M=25MB/sec and R=2MB/sec

S= 250/23= 11sec.

DIFFERENCE BETWEEN LEAKY BUCKET AND TOKEN BUCKET ALGORITHM

TOKEN BUCKET	**LEAKY BUCKET**
Token dependent.	Token independent.
If bucket is full token are discarded, but not the packet.	If bucket is full packet or data is discarded.
Packets can only transmitted when there are enough token	Packets are transmitted continuously.
It allows large bursts to be sent faster rate after that constant rate	It sends the packet at constant rate
It saves token to send large bursts.	It does not save token.

Packet Scheduling

- Algorithms that allocate router resources among the packets of a flow and between competing flows are called packet scheduling algorithms.
- Three different kinds of resources can potentially be reserved for different flows:

1. Bandwidth.
2. Buffer space.
3. CPU cycles.

Bandwidth reservation

- Making sure the bandwidth of input line and output line are fair enough to handle the traffic.

For example: If a flow requires 1 Mbps and the outgoing line has a capacity of 2 Mbps, trying to direct three flows through that line is not going to work.

Buffer Space

- The packet is buffered inside router until it is transmitted.
- Purpose of buffer is to absorb small bursts of traffic.
- For good quality of service, some buffers might be reserved for a specific flow so that flow does not have to compete for buffers with other flows.

CPU cycles

- Routers CPU time is used to process a packet.
- Some kinds of packets require greater CPU processing, such as the ICMP packets.
- It should be made sure that the CPU is not overloaded to ensure timely processing of the packets.

CPU cycles

Computing CPU utilization :

Mean arrival rate of packets- λ packets/sec.

Mean processing capacity of packets- μ packets/sec.

Delay experienced by a packet:

$T= 1/ \mu \ * 1/ (1- \lambda / \mu)$

$= 1/ \mu \ * 1/ (1- \rho)$

Where $\rho = \lambda/\mu$ *is CPU utilization.*

For example,

if λ = 950,000 packets/sec

μ = 1,000,000 packets/sec

ρ =0.95

Delay experienced by each packets:

T= 20μsec instead of 1 μsec.

- This time accounts for both the queueing time and the service time, as can be seen when the load is very low.
- If there are, say, 30 routers along the flow's route, queueing delay alone will account for 600 μsec of delay.

- Packet scheduling algorithms allocate bandwidth and other router resources by determining which of the buffered packets to send on the output line next.

FIFO(First In First Out) or FCFS (First Come First Serve)

- Each router buffers packets in a queue for each output line until they can be sent, and they are sent in the same order that they arrived.

- FCFS routers usually drop newly arriving packets when the queue is full.
  – **Tail Drop.**
- FCFS scheduling is simple to implement, not suited for providing good QOS when there are multiple flows.
- If one of the flow is aggressive and send the packets very fast other flows will starve for the service.

Fair Queuing algorithm

- The routers have separate queues, one for each flow for a given output line.
- The router scans the queues round-robin format.

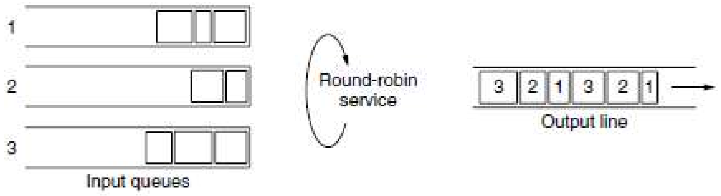


Figure 5-30. Round-robin fair queueing.

- With n hosts competing for the output line, each host gets to send one out of every n packets.
- It is fair in the sense that all flows get to send packets at the same rate.

- Drawback: more bandwidth is given to hosts that use large packets than to hosts that use small packets.
- Use byte-by-byte round-robin, instead of a packet-by-packet round-robin.
- This algorithm gives same priority to all the hosts.
- To assign priority for some applications a variant of this algorithm- Weighted Fair Queuing(WFQ) is used.
- Other scheduling algorithms – Round robin, priority scheduling.

- Packet scheduling algorithms allocate bandwidth and other router resources by determining which of the buffered packets to send on the output line next.

FIFO(First In First Out) or FCFS (First Come First Serve)

- Each router buffers packets in a queue for each output line until they can be sent, and they are sent in the same order that they arrived.

- FCFS routers usually drop newly arriving packets when the queue is full. – **Tail Drop.**
- FCFS scheduling is simple to implement, not suited for providing good QOS when there are multiple flows.
- If one of the flow is aggressive and send the packets very fast other flows will starve for the service.

Fair Queuing algorithm

- The routers have separate queues, one for each flow for a given output line.
- The router scans the queues round-robin format.

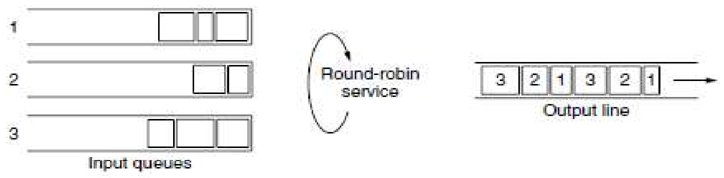


Figure 5-30. Round-robin fair queueing.

- With n hosts competing for the output line, each host gets to send one out of every n packets.
- It is fair in the sense that all flows get to send packets at the same rate.

- Drawback: more bandwidth is given to hosts that use large packets than to hosts that use small packets.
- Use byte-by-byte round-robin, instead of a packet-by-packet round-robin.
- This algorithm gives same priority to all the hosts.
- To assign priority for some applications a variant of this algorithm- Weighted Fair Queuing(WFQ) is used.
- Other scheduling algorithms – Round robin, priority scheduling.

Admission Control

- The user offers a flow with an accompanying QoS requirement to the network.
- The network then decides whether to accept or reject the flow based on its capacity and the commitments it has made to other flows.
- If it accepts, the network reserves capacity in advance at routers to guarantee QoS when traffic is sent on the new flow.

- The reservations must be made at all of the routers along the route that the packets take through the network.
- Any routers on the path without reservations might become congested, and a single congested router can break the QoS guarantee.
- QoS guarantees for new flows may still be accommodated by choosing a different route for the flow that has excess capacity. This is called **QoS routing.**

- Flow specification- Describing a flow accurately in terms of specific parameters.

Parameter	Unit
Token Bucket Rate	Bytes/sec
Token Bucket Size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

Integrated and Differentiated services

- The two principle approaches to applying QoS mechanisms are Integrated Services (IntServ) and Differentiated Services (DiffServ).
- The generic name for such services are: flow-based algorithms or integrated services.
- It was aimed at both unicast and multicast applications.
- An example of unicast is a single user streaming a video clip from a news site.
- An example of multicast is a collection of digital television stations broadcasting their programs as streams of IP packets to many receivers at various locations.

IntServ

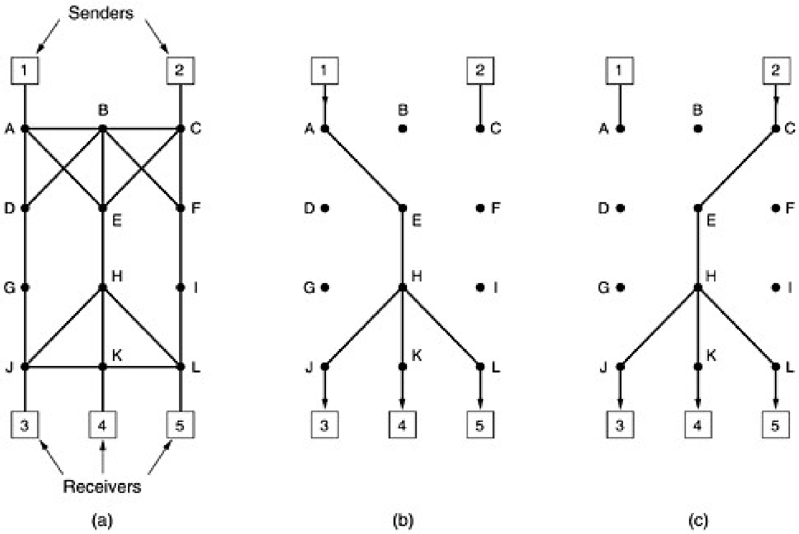
- The IntServ approach involves the reservation of bandwidth on the network from end to end between two communicating devices, before communication begins.
- This is achieved using the Resource Reservation Protocol (RSVP).
- Once the reservation is acquired, the communication takes place.
- When completed, the network resources are relinquished to be used by other applications and services.

RSVP – Resource Reservation Protocol

- **This protocol is used for making the reservations**; other protocols are used for sending the data.
- The protocol uses multicast routing using spanning trees.
- Each group is assigned a group address.
- To send to a group, a sender puts the group's address in its packets.
- The standard multicast routing algorithm then builds a spanning tree covering all group members.
- The **routing algorithm is not part of RSVP**.

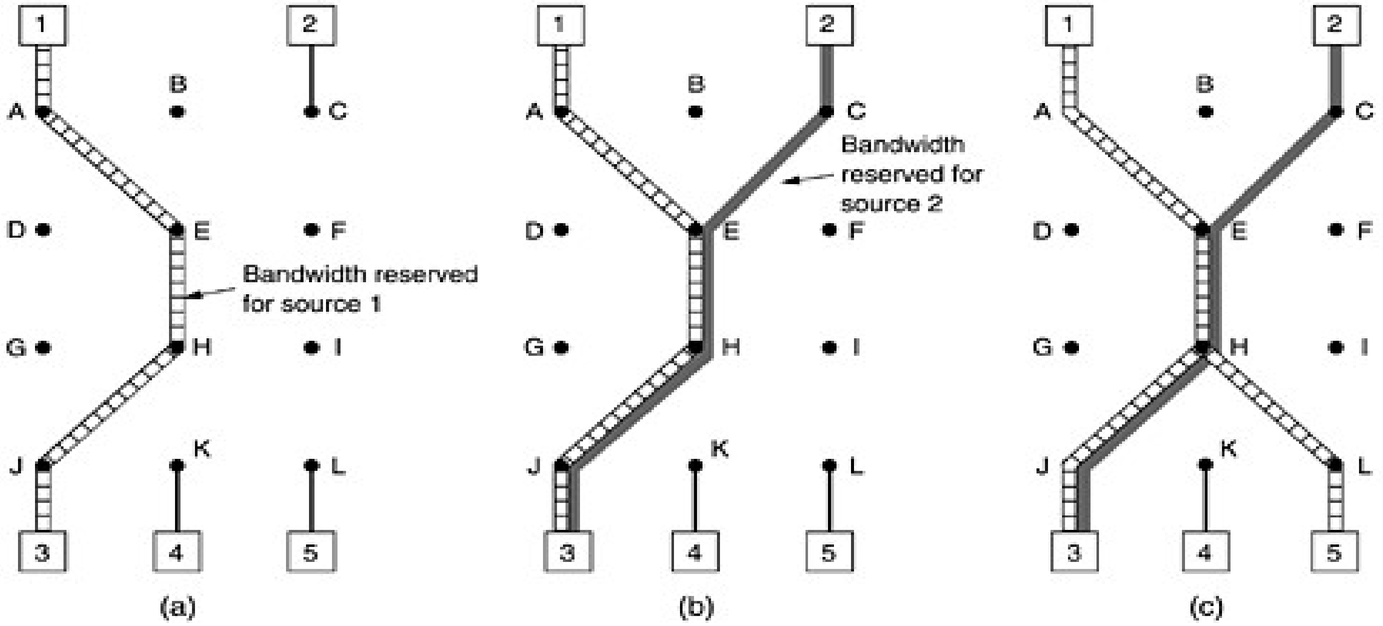
Consider a network, Hosts 1 and 2 are multicast senders, and hosts 3, 4, and 5 are multicast receivers.

- The senders and receivers are disjoint, but in general, the two sets may overlap.
- The multicast trees for hosts 1 and 2 are shown

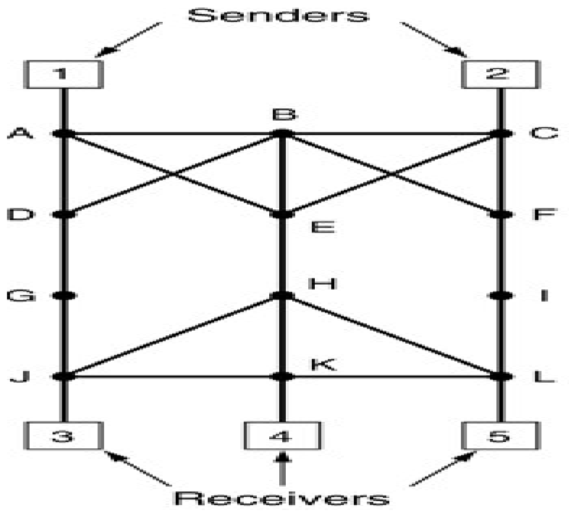


- Any of the receivers in a group can send a reservation message up the tree to the sender.
- The message is propagated using the reverse path forwarding algorithm.
- At each hop, the router notes the reservation and reserves the necessary bandwidth
- If insufficient bandwidth is available, it reports back failure.
- By the time the message gets back to the source, bandwidth has been reserved all the way from the sender to the receiver making the reservation request along the spanning tree.

- Here host 3 has requested a channel to host 1
- Once it has been established, packets can flow from 1 to 3 without congestion.
- If host 3 next reserves a channel to the other sender, host 2, so the user can watch two television programs at once.


1
2
A
B
C
D
E
F
G
H
I
J
K
L
3
4
5
Bandwidth reserved for source 1
(a)
Bandwidth reserved for source 2
(b)
(c)

- Host 5 decides to watch the program being transmitted by host 1 and also makes a reservation.
- First, dedicated bandwidth is reserved as far as router H, later router sees that it already has a feed from host 1, so if the necessary bandwidth has already been reserved, it does not have to reserve any more.
- Note that hosts 3 and 5 might have asked for different amounts of bandwidth (e.g., 3 has a small screen and 5 a bigger one with higher resolution).
- The capacity reserved must be large enough to satisfy the greediest receiver.



Bandwidth reserved in Bps

A	**2**
B	**0**
C	**1**
E	**3**
H	**3**
J	**3**
K	**2**
L	**1**

For given network topology,

R3 requests bandwidth 2 MBps from S1

R3 requests bandwidth 1 MBps from S2

R4 requests bandwidth 2 MBps from S1

R5 requests bandwidth 1 MBps from S2

What is the bandwidth required to be reserved at Routers A, B, C, E, H, J, K, L ?

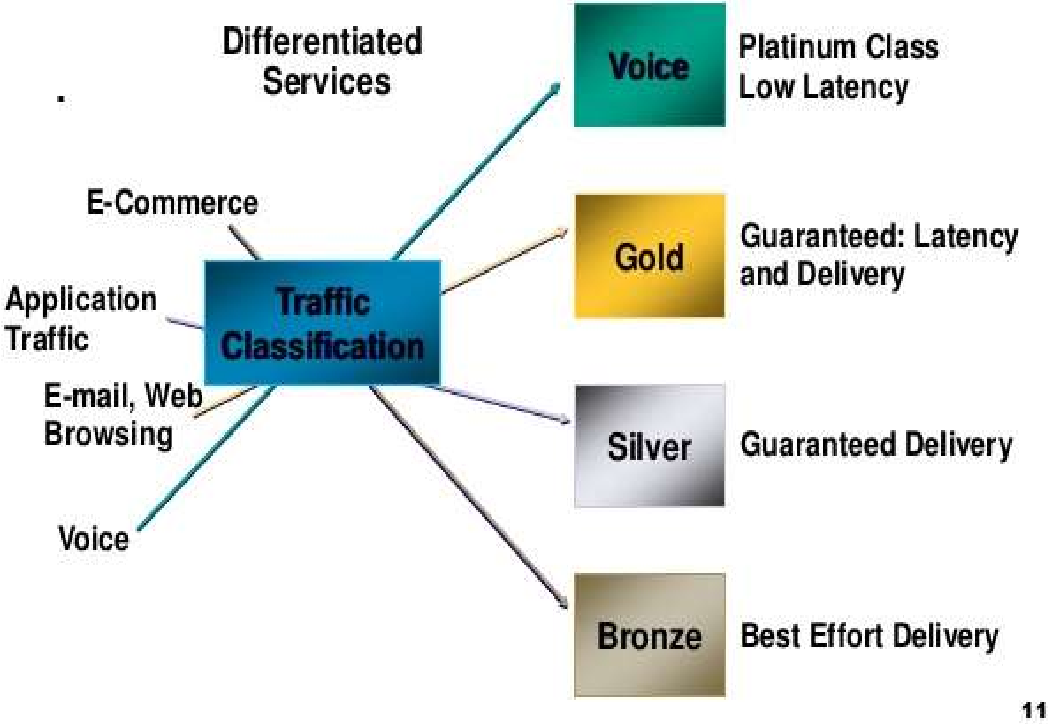
Drawbacks of IntServ

- All routers within a network must be configured to support and respond to RSVP requests, if only one fails, the reservation will fail.
- There may potentially be hundreds or even thousands of individual reservation requests for routers to create, maintain and tear down reservations on demand, a process that can quickly overwhelm the CPU and memory of the RSVP-enabled routers.
- Because RSVP will reserve the bandwidth from end to end, no other service can use that bandwidth, even under conditions of extreme congestion.

DiffServ

- DiffServ is a QoS approach involving packet prioritization.
- With DiffServ, individual packets are marked according to the type of prioritization they require.
- Routers and switches use various queueing strategies to conform to these requirements.
- This approach is known as **class-based** (as opposed to flow-based) quality of service.

Differentiated service goal is to divide the traffic into classes



- Differentiated services (DS) can be offered by a set of routers forming an administrative domain e.g ISP
- The administration defines a **set of service classes** with corresponding **forwarding rules.**
- If a customer signs up for DS, customer packets entering the domain may carry a Type of Service field in them, with better service provided to some classes (e.g., premium service) than to others.
- This scheme requires no advance setup, no resource reservation, and no time-consuming end-to-end negotiation for each flow, as with integrated services.
- This makes DS relatively easy to implement.

Types of forwarding

- **Expedited forwarding**
- **Assured Forwarding**

Expedited Forwarding:

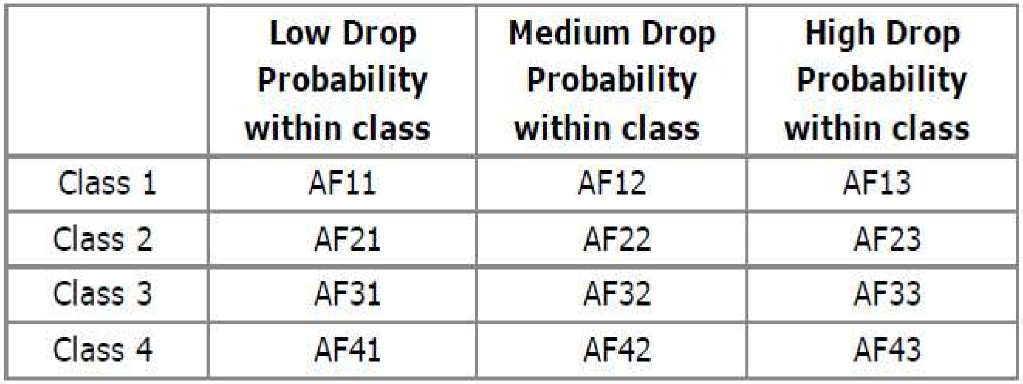
The vast majority of the traffic is expected to be regular, but a limited fraction of the packets are expedited.

- The expedited packets should be able to transit the network as though no other packets were present.
- In this way they will get low loss, low delay and low jitter service—just what is needed for VoIP.
- Packets are classified as expedited or regular and marked accordingly.
- This step might be done on the sending host or in the ingress (first) router.

- If the marking is done by the host, the ingress router is likely to police the traffic to make sure that customers are not sending more expedited traffic than they have paid for.
- Within the network, the routers may have two output queues for each outgoing line, one for expedited packets and one for regular packets.
- When a packet arrives, it is queued accordingly.
- The expedited queue is given priority over the regular one, for example, by using a priority scheduler.
- In this way, expedited packets see an unloaded network, even when there is, in fact, a heavy load of regular traffic.

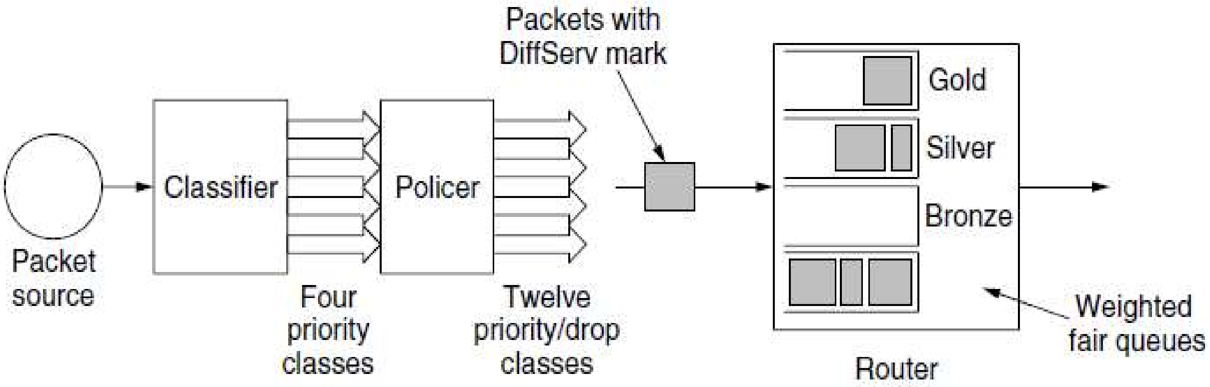
Assured Forwarding

- Assured forwarding specifies that there shall be four priority classes, each class having its own resources.
- The top three classes might be called gold, silver, and bronze.
- In addition, it defines three discard classes for packets that are experiencing congestion: low, medium, and high.
- Taken together, these two factors define 12 service classes.



	Low Drop Probability within class	Medium Drop Probability within class	High Drop Probability within class
Class 1	AF11	AF12	AF13
Class 2	AF21	AF22	AF23
Class 3	AF31	AF32	AF33
Class 4	AF41	AF42	AF43

Implementation of assured forwarding



- The first step is to classify the packets into one of the four priority classes.
- The next step is to determine the discard class for each packet.
- Finally, the packets are processed by routers in the network with a packet scheduler that distinguishes the different classes.