UNIT IV
Asynchronous Transfer Mode (ATM)

Why ATM networks?

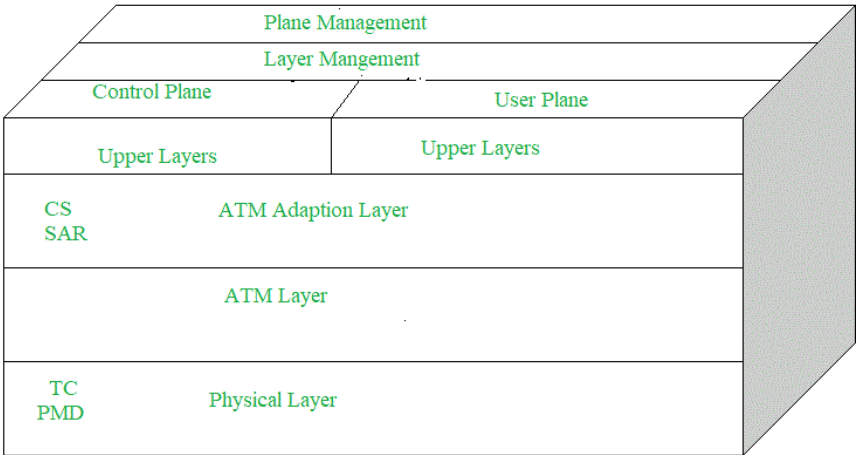
1. Driven by the integration of services and performance requirements of both telephony and data networking: "broadband integrated service vision" (B-ISON). Telephone networks support a single quality of service and are expensive to boot. Internet supports no quality of service but is flexible and cheap. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM):

It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.
ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with **end-to-end** quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

ATM Layers:



1. **ATM Adaption Layer (AAL) –** It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and

segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

2. **Physical Layer –**
   It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:
   - It converts cells into a bitstream.
   - It controls the transmission and receipt of bits in the physical medium.
   - It can track the ATM cell boundaries.
   - Look for the packaging of cells into the appropriate type of frames.
3. **ATM Layer –**
   It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

ATM Applications:

1. **ATM WANs –** It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

2. **Multimedia virtual private networks and managed services –** It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.

3. **Frame relay backbone –** Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.

4. **Residential broadband networks –** ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

5. **Carrier infrastructure for telephone and private line networks –** To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

ATM PROTOCOL ARCHITECTURE

4.1 What is ATM protocol architecture?

The *asynchronous transfer mode* (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.

Figure 24 shows the reference model for ATM. The first thing to notice is that, as well as layers, the model has planes. The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes.

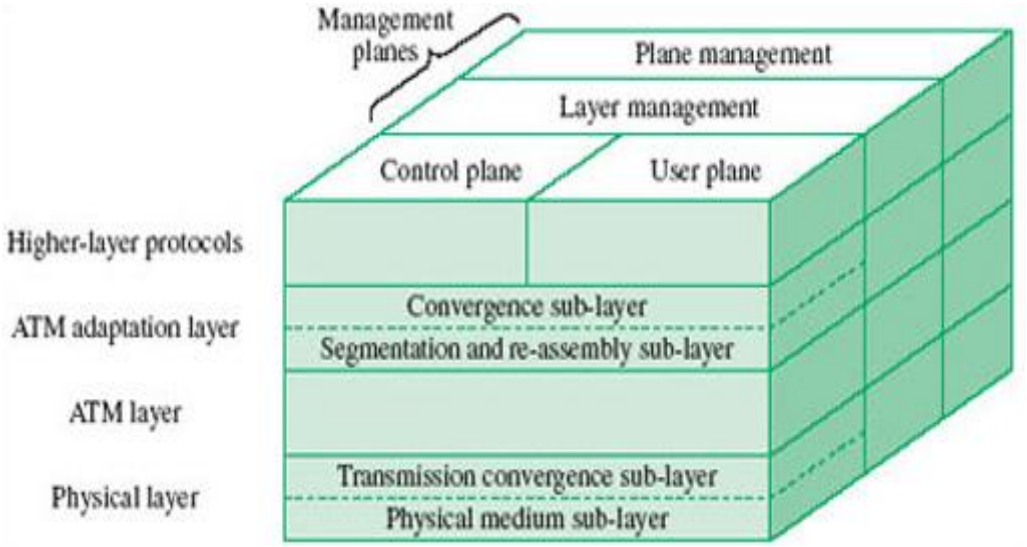


Figure: ATM reference model

The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. The horizontal layers indicate the encapsulation of protocols through levels of abstraction as one layer is built on top of another, whereas the vertical planes indicate the functions that require co-ordination of the actions taken by different layers. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane).

The protocols in the ATM layer provide communication between ATM switches while the protocols in the ATM adaptation layer (AAL) operate end-to-end between users. This is illustrated in the example ATM network in Figure 25.

Two types of interface are identified in Figure 24: one between the users and the network (user-network interface), and the other between the nodes (switches) within the network (network-node interface).

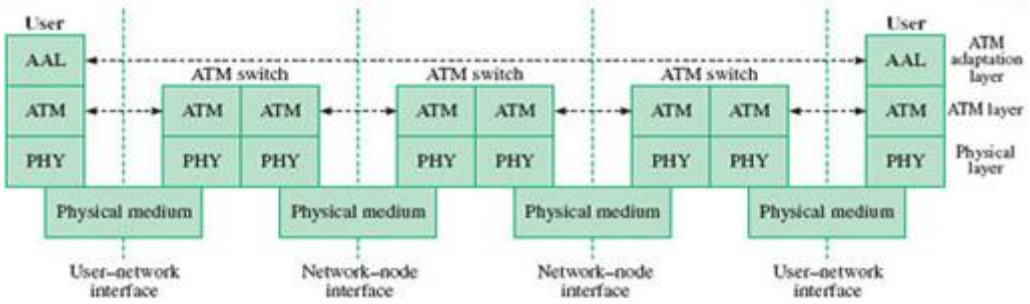
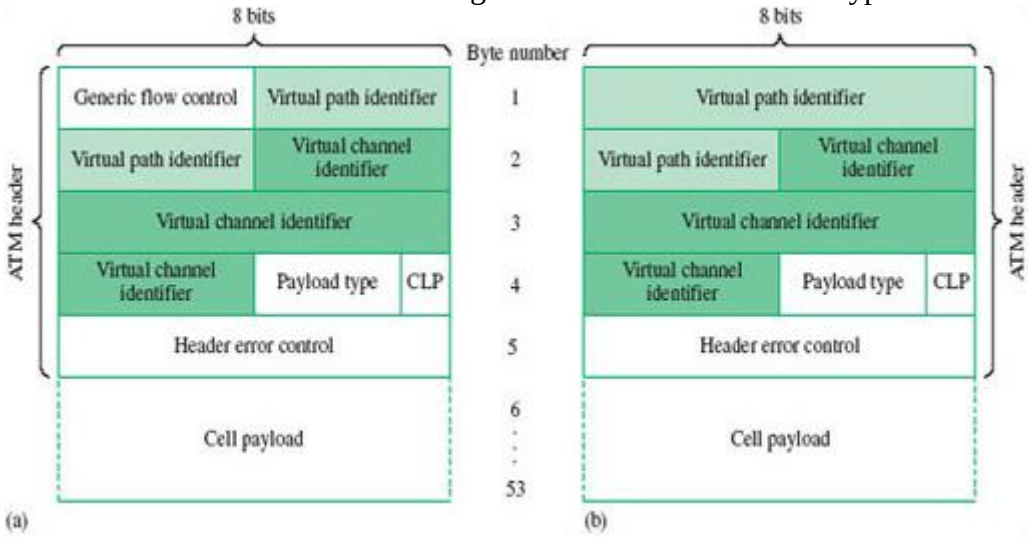


Figure 25 ATM network

Before describing the functions of the three layers in the ATM reference model, I shall briefly describe the format of ATM cells. Figure 26 shows the two basic types of cell.



View larger image

Figure 26 (a) ATM cells at the user-network interface; (b) ATM cells at the network-node interface Each ATM cell consists of 53 bytes: the header is five bytes long and the remaining 48 bytes (the cell payload) carry information from higher layers. The only difference between the two types of ATM cell is that the cells at the user-network interface carry a data field for the flow control of data from users. This means that only eight bits are available for virtual path identifiers, rather than 12 bits at the network-node interface.

ATM LOGICAL CONNECTION

Logical connections in ATM are referred to as virtual channel connections (VCCs). A VCC is analogous to a virtual circuit in X.25; it is the basic unit of switching in an ATM network. A VCC is set up between two end users through the network and a variable-rate, full-duplex flow of fixed-size cells is exchanged over the connection. VCCs are also used for user-network exchange (control signaling) and network-network exchange (network management and routing). For ATM, a second sublayer of processing has been introduced that deals with the concept of virtual path (Figure 1). A virtual path connection (VPC) is a bundle of VCCs that have the same endpoints. Thus, all of the cells flowing over all of the VCCs in a single VPC are switched together.

The virtual path concept was developed in response to a trend in high-speed networking in which the control cost of the network is becoming an increasingly higher proportion of the overall network cost. The virtual path technique helps contain the control cost by grouping connections sharing common paths through the network into a single unit.

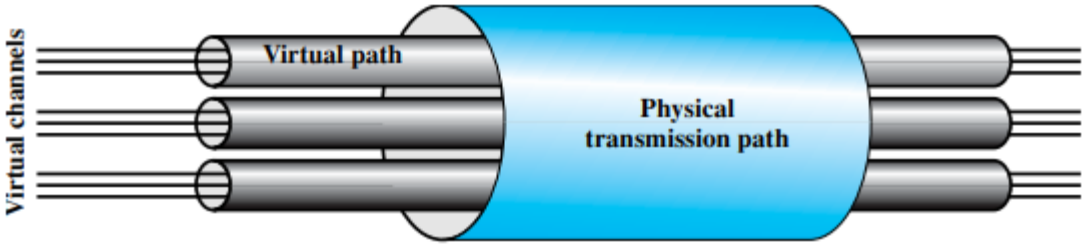


Fig.1 ATM Connection Relationships

Advantages of virtual path

1. Simplified network architecture: Network transport functions can be separated into those related to an individual logical connection (virtual channel) and those related to a group of logical connections (virtual path).

2. Increased network performance and reliability: The network deals with fewer, aggregated entities.

3. Reduced processing and short connection setup time: Much of the work is done when the virtual path is set up. By reserving capacity on a virtual path connection in anticipation of later call arrivals, new virtual channel connections can be established by executing simple control functions at the endpoints of the virtual path connection; no call processing is required at transit nodes. Thus, the addition of new virtual channels to an existing virtual path involves minimal processing.

4. Enhanced network services: The virtual path is used internal to the network but is also visible to the end user. Thus, the user may define closed user groups or closed networks of virtual channel bundles.

Figure 2 suggests in a general way the call establishment process using virtual channels and virtual paths. The process of setting up a virtual path connection is decoupled from the process of setting up an individual virtual channel connection,

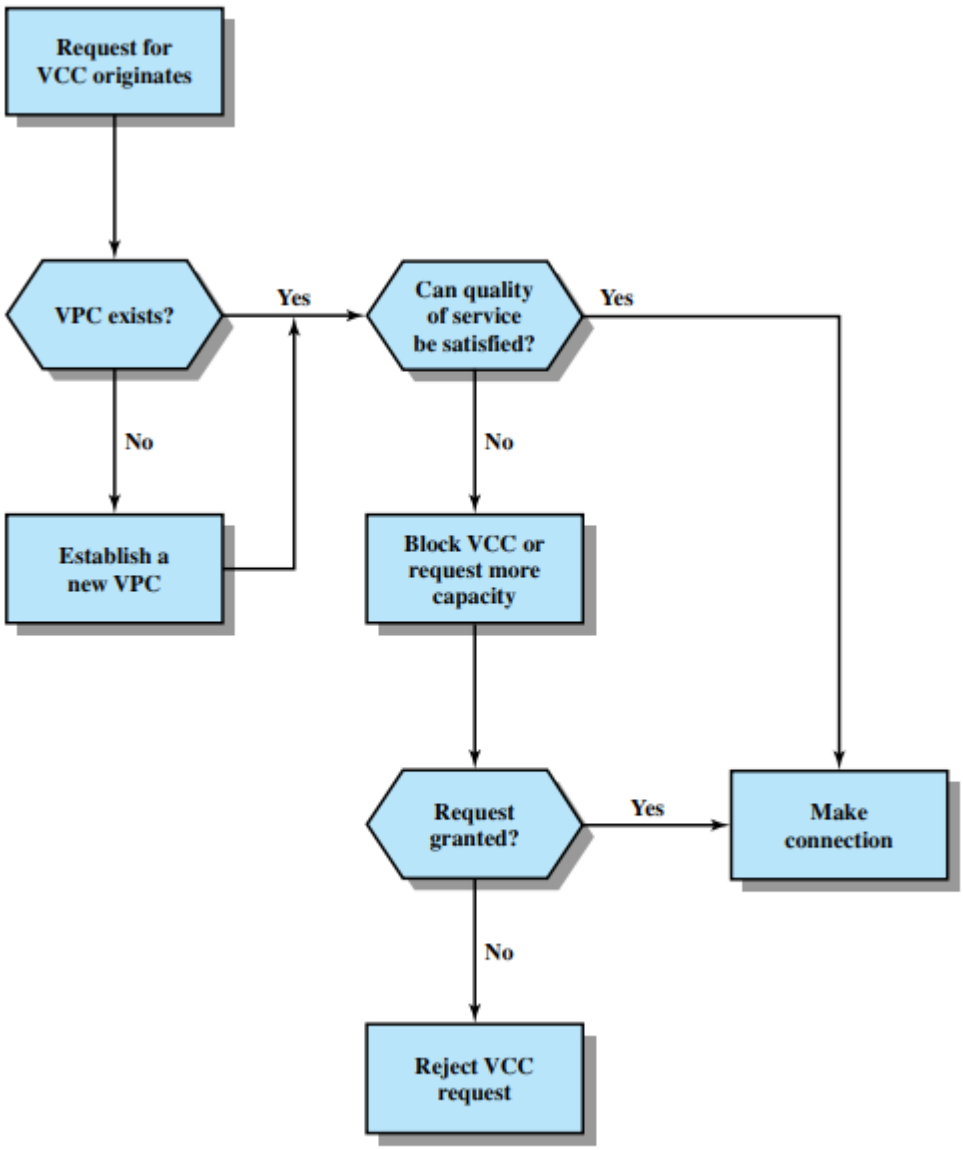
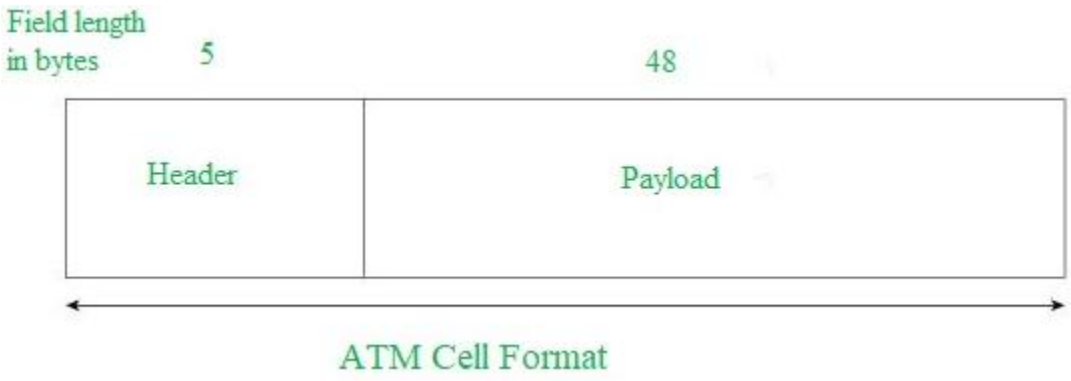


Fig.1 Call Establishent Using Virtual Paths

- The virtual path control mechanisms include calculating routes, allocating capacity, and storing connection state information.
- To set up a virtual channel, there must first be a virtual path connection to the required destination node with sufficient available capacity to support the virtual channel, with the appropriate quality of service. A virtual channel is set up by storing the required state information (virtual channel/virtual path mapping).

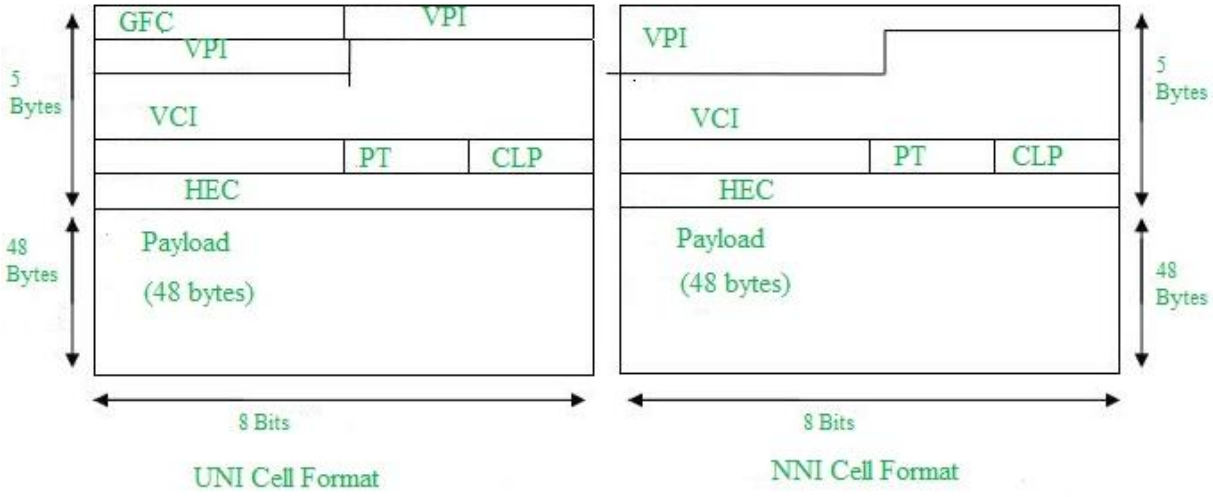
ATM CELL

ATM Cell Format – As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Asynchronous Transfer Mode can be of two format types which are as follows:



1. **UNI Header:** This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

TRANSMISSION OF ATM CELL

Working of ATM: ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of

major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.
Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

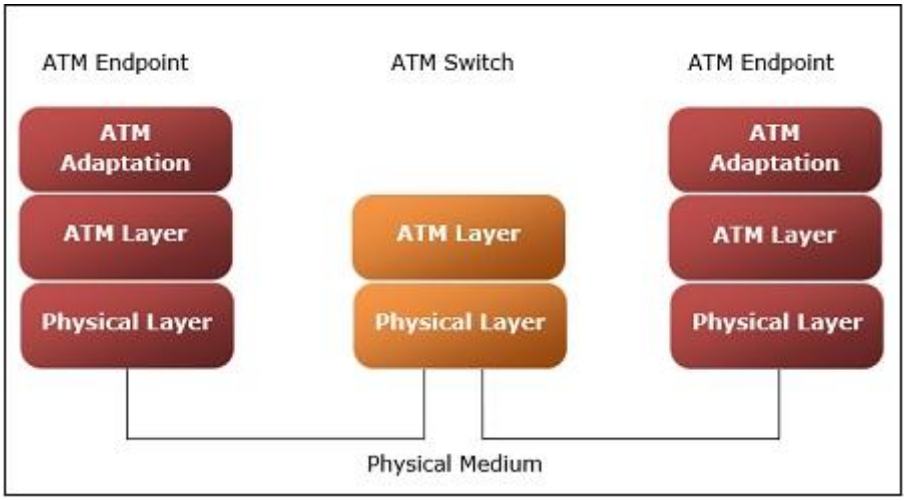
ATM vs DATA Networks (Internet) –

- ATM is a "virtual circuit" based: the path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.

- ATM Cells: Fixed or small size and Tradeoff is between voice or data. While IP packets are of variable size.

- Addressing: ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.

The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload. There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.



Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

- **Physical Layer** − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
- **ATM Layer** −This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL)** −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer.
- **ATM endpoints** − It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
- **ATM switch** −It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

ATM SERVICE CATEGORIES

Quality of Service (QoS) is a type of Networking Technology that can guarantee a specific level of output for a specific connection, path, or type of traffic. QoS mechanisms provide control on both quality and availability of bandwidth whereas another network provides only a best-effort delivery.

QoS feature is used when there is traffic congestion in-network, it gives priority to certain real-time media. A high level of QoS is used while transmitting real-time multimedia to eliminate latency and dropouts. Asynchronous Transfer Mode (ATM) is a networking technology that uses a certain level of QoS in data transmission.

The Quality of Service in ATM is based on following: Classes, User-related attributes, and Network-related attributes.

These are explained as following below.

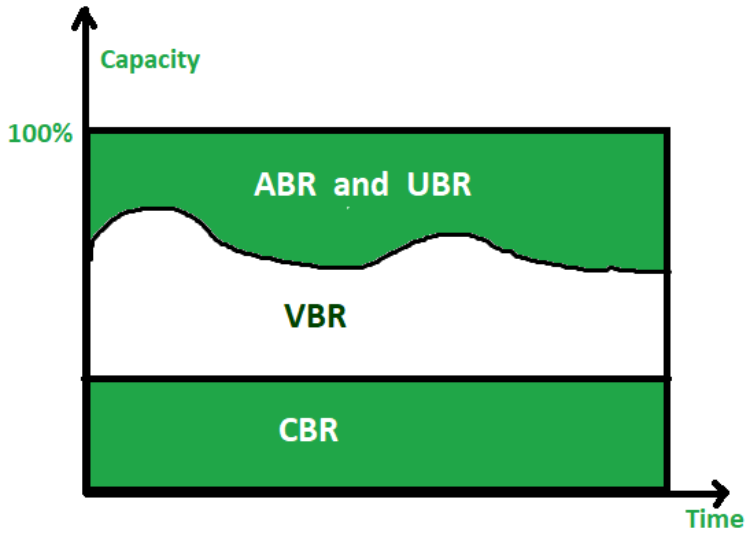
1. Classes :

The ATM Forum defines four service classes that are explained below –

1. **Constant Bit Rate (CBR) –**
   CBR is mainly for users who want real-time audio or video services. The service provided by a dedicated line. For example, T line is similar to CBR class service.
2. **Variable Bit Rate (VBR) –**
   VBR class is divided into two sub classes –
   - **(i) Real-time (VBR-RT) :**
     The users who need real-time transmission services like audio and video and they also use compression techniques to create a variable bit rate, they use VBR-RT service class.
   - **(ii) Non-real Time (VBR-NRT) :**
     The users who do not need real-time transmission services but they use

compression techniques to create a variable bit rate, then they use VBR-NRT service class.

3. **Available Bit Rate (ABR) –**
   ABR is used to deliver cells at a specific minimum rate and if more network capacity is available, then minimum rate can be exceeded. ABR is very much suitable for applications that have high traffic.
4. **Unspecified Bit Rate (UBR) –**
   UBR class and it is a best-effort delivery service that does not guarantee anything.



The above diagram shows relationship of different classes to total capacity of network.

2. User Related Attributes :
ATM defines two sets of attributes and User-related attribute is one of them. They are those type attributes that define at what speed user wants to transmit data. These are negotiated during time of contract between a network and a customer.
The following are some user-related attributes –

1. **Sustained Cell Rate (SCR) –**
   SCR is average cell rate over a long time interval. The original cell rate can be less or greater than value of SCR, but average must be equal to or less than value of SCR.
2. **Peak Cell Rate (PCR) –**
   PCR is defined as maximum cell rate of sender. As long as SCR is maintained, cell rate of user can reach this peak value.
3. **Minimum Cell Rate (MCR) –**
   MCR defines minimum cell rate acceptable to sender. For example, if MCR is 50,000, network must guarantee that sender can send at least 50,000 cells per second.
4. **Cell Variation Delay Tolerance (CVDT) –**
   CVDT is a measure of the variation in cell transmission times. Let’s take an example if value of CVDT is 8 ns, this signifies that difference between minimum and maximum delays in delivering the cells should not be greater than 8 ns.

3. Network-Related Attributes

The attributes that are used to define different characteristics of network are known as Network-related attributes.

The following are some network-related attributes –

1. **Cell Loss Ratio (CLR) –**
   CLR defines the fraction of cells lost (or delivered so late that they are considered lost) during transmission. For example, if sender sends 100 cells and one of them is lost, CLR is
   CLR = 1/100
2. **Cell Transfer Delay (CTD) –**
   The average time taken by a cell for traveling from source to destination is known as Cell transfer delay. The maximum CTD and minimum CTD are also considered attributes.
3. **Cell Delay Variation (CDV) –**
   CDV is difference between CTD maximum and CTD minimum.
4. **Cell Error Ratio (CER) –**
   CER defines fraction of cells delivered in error

CONGESTION CONTROL IN DATA NETWORKS

Network Congestion occurs when the traffic flowing through a network exceeds its maximum capacity. In most cases, congestion is a temporary issue with the network caused due to a sudden upsurge of traffic, however, sometimes, a network is continually congested, indicating a deeper problem. End-users perceive network congestion as Network Slowdown or a very large delay in processing requests.

Network congestion is also a contributing factor in the following underlying issues:

- **High Latency –**
  In a congested network, the time taken by a packet to reach its destination increases significantly, hence a higher latency rate is observed.
- **Connection timeouts –**
  Ideally, the service should wait for the arrival of packets but in several cases, the connection terminates due to timeout.
- **Packet loss –**
  Many packets cannot reach their destination if the network is congested, and will be dropped eventually due to timeout.

Causes of network congestion :

1. **Excessive bandwidth consumption –**
   Certain users or devices on the network may occasionally utilize more bandwidth than the average user or device. This can put a strain on the network and its routing equipment (routers, switches, and cables), causing network congestion.

2. **Poor subnet management –**
   For better resource management, a big network is divided into subnets. However, network congestion could arise if the subnets are not scaled according to usage patterns

and resource requirements.

3. **Broadcast Storms –**
   A broadcast storm occurs when there is a sudden upsurge in the number of requests to a network. As a result, a network may be unable to handle all of the requests at the same time.

4. **Multicasting –**
   Multicasting occurs when a network allows multiple computers to communicate with each other at the same time. In multicasting, a collision can occur when two packets are sent at the same time. Such frequent collisions may cause a network to be congested.

5. **Border Gateway Protocol –**
   All traffic is routed by BGP via the shortest possible path. However, while routing a packet, it doesn't consider the amount of traffic present in the route. In such scenarios, there is a possibility all the packets are being routed via the same route which may lead to network congestion.

6. **Too many devices –**
   Every network has a limit on the amount of data it can manage. This capacity establishes a limit on how much bandwidth and traffic your network can handle before performance degrades. If the network has too many devices linked to it, the network may become burdened with data requests.

7. **Outdated Hardware –**
   When data is transmitted over old switches, routers, servers, and Internet exchanges, bottlenecks can emerge. Data transmission can get hampered or slowed down due to outdated hardware. As a result, network congestion occurs.

8. **Over-subscription –**
   A cost-cutting tactic that can result in the network being compelled to accommodate far more traffic than it was designed to handle (at the same time).

EFFECTS OF NETWORK CONGESTION :

1. Queueing delay
2. Packet Loss
3. Slow Network
4. Blocking of new connections
5. Low throughput

Test for network congestion :

- Run Command Prompt as administrator.
- Type **tracert google.com** in the CMD window.

```
Administrator: Command Prompt

C:\Windows\system32> tracert google.com

Tracing route to google.com [172.217.166.14]
over a maximum of 30 hops:

  1     2 ms     3 ms     2 ms  dsldevice.lan [192.168.1.1]
  2     7 ms     4 ms     4 ms  abts-north-static-070.127.176.122.airtelbroadband.in [122.176.127.70]
  3     5 ms     4 ms     4 ms  125.19.38.109
  4     4 ms     5 ms     5 ms  116.119.42.210
  5     5 ms     5 ms     4 ms  72.14.217.194
  6     5 ms     5 ms     5 ms  172.253.69.191
  7     7 ms     6 ms     5 ms  209.85.251.231
  8     9 ms     7 ms    12 ms  del03s17-in-f14.1e100.net [172.217.166.14]

Trace complete.

C:\Windows\system32>
```

Tracert

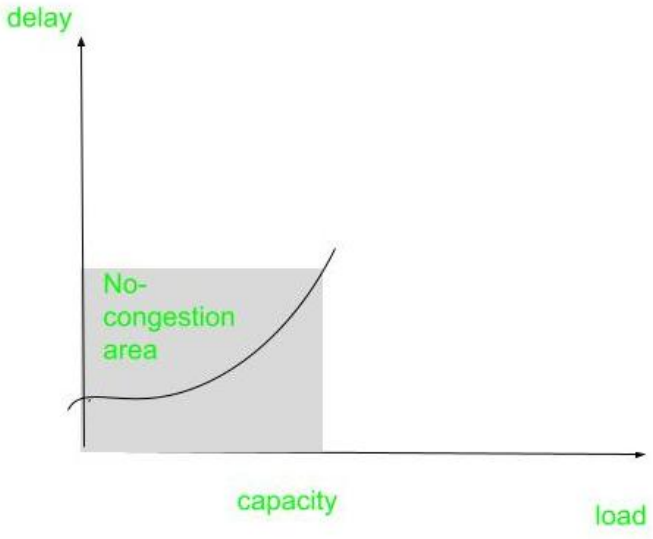
- Take note of how many hops it takes to get to the final server.
- For every hop, check out the value of ping.

Congestion at the network layer is related to two issues, throughput and delay.

1. Based on delay

When the load is much less than the capacity of the network, the delay is at a minimum . This minimum delay is composed of propagation delay and processing delay, both of which are negligible.

However, when the load reaches the network capacity ,the delay increases sharply because we now need to add the queuing delay to the total delay. The delay becomes infinite when the load is greater than the capacity.



delay as a function load

2. Based on Throughout

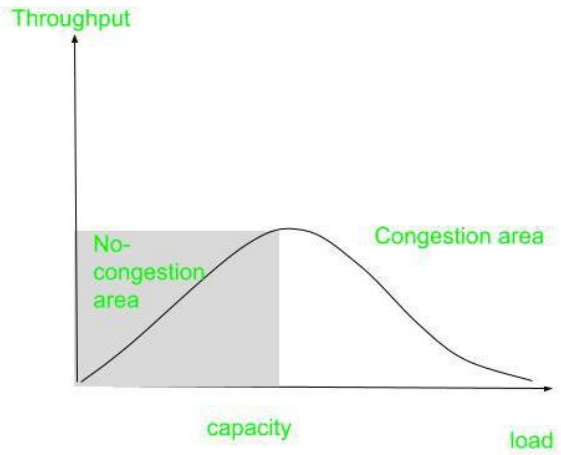
When the load is below the capacity of the network, the throughput increases proportionally with the load.

We expect the throughput to remain constant after the load reaches the capacity, but instead the throughput declines sharply.

The reason is the discarding of packets by the routers.

When the load exceeds the capacity, the queues become full and the routers have to discard some packets.

Discarding packets does not reduce the number of packets in the network because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destinations.



throughput as a function of delay

How to fix network congestion?

1. Divide your network into subnets that can be resized to meet traffic.
2. TCP/IP settings should be adjusted to balance packet send/request speeds.
3. Use a CDN (Content Delivery Network) to save time by directing more requests to edge servers.
4. Choke packets are used to reduce the output of sender devices, which helps to avoid network congestion.
5. In case the default route becomes congested, you can employ multi-hop routing so that traffic can be managed.
6. Upgrade your Internet plan to allow for more devices and increased bandwidth. Check to see if your devices are up to date and not outdated (even the cables).

CONGESTION CONTROL

Congestion control algorithms

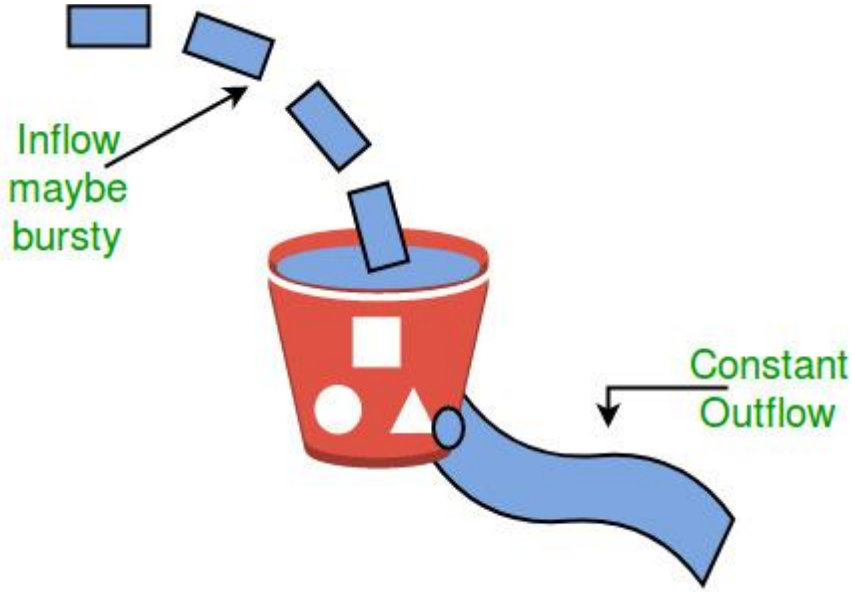
- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.

- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithm which are as follows:

- **Leaky Bucket Algorithm**
- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

- **Token bucket Algorithm**
- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.

- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

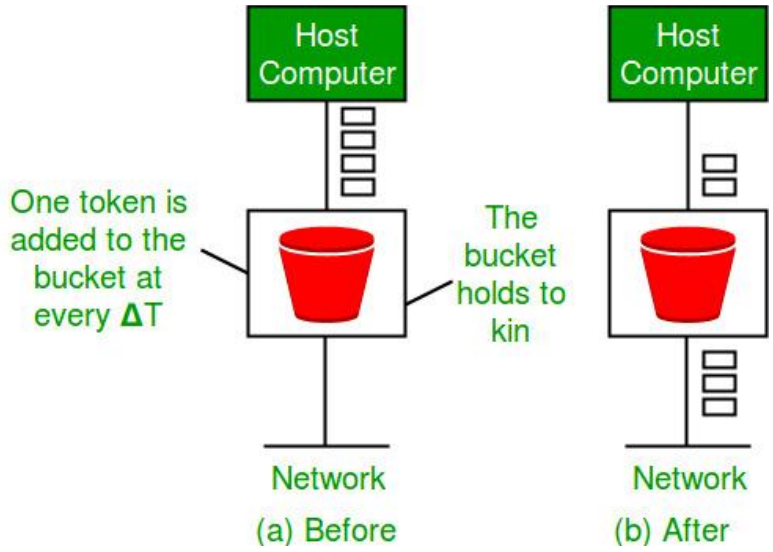
1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Ways in which token bucket is superior to leaky bucket: The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: $M * s = C + \rho * s$ where S – is time taken M – Maximum output rate ρ – Token arrival rate C – Capacity of the token bucket in byte
Let's understand with an example,



TRAFFIC MANAGEMENT

Traffic shaping is used to control bandwidth of the network to ensure quality of service to business-critical applications. It can be validated at :

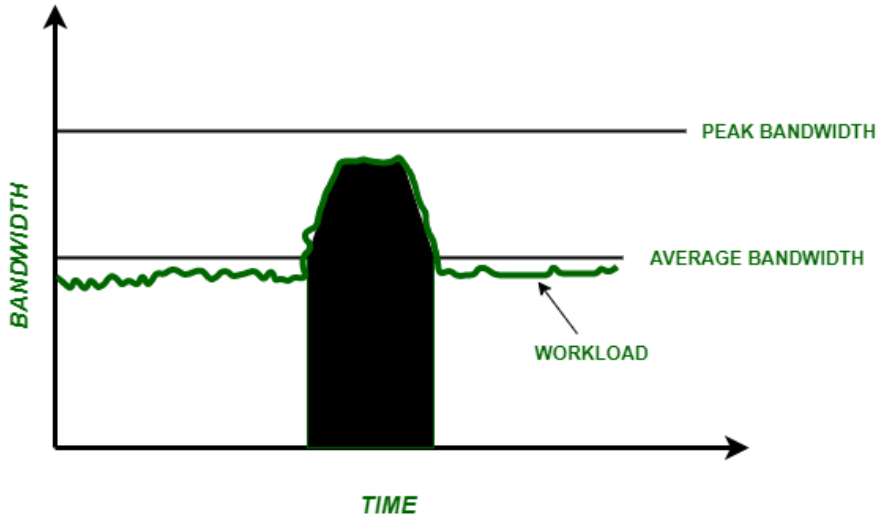
1. Port group level
2. Virtual or distributed virtual switch

This technique uses three parameters to shape the flow of network traffic :

1. Burst size
2. Average bandwidth
3. Peak bandwidth

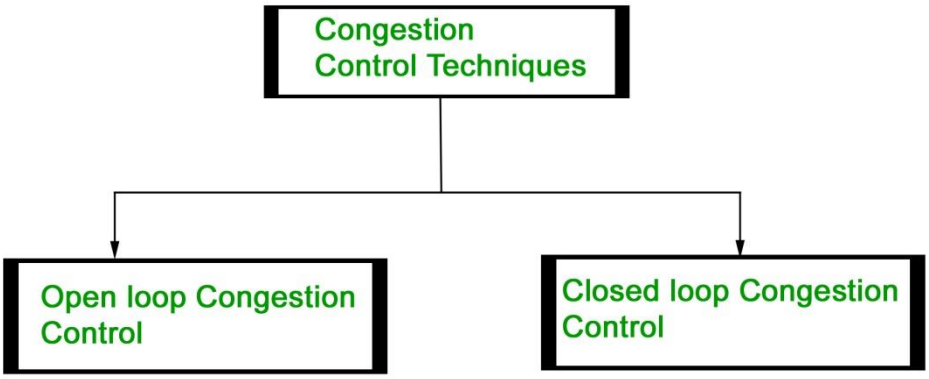
These are explained as following below.

1. **Burst Size :**When the workload is greater than average bandwidth it is known as burst. Maximum amount of bytes that are permitted to move in a burst are defined by burst size.
   Burst Size = Time*Bandwidth
   Bandwidth can increase up to peak bandwidth. Available bandwidth and time burst can stay for a specific burst size are inversely proportional to each other. Therefore, greater time burst can stay for a specific burst size, lesser is available bandwidth and vice versa. If a particular burst is greater than the configured burst size, then remaining frames will be lined up for later transmission. The frames will be discarded in case queue is full.
2. **Average Bandwidth :**It is configured to set permitted bits per second across a port group level or a virtual/distributed virtual switch, over time. The rate of data transfer is permitted over time.
3. **Peak bandwidth :**It decides maximum number of bits per second permitted across a port group level or a virtual/distributed virtual switch without discarding or queuing the frames.
   Peak Bandwidth > Average Bandwidth



Traffic Shaping : A network traffic management technique.
Example : Suppose we have Burst Size = 3 Kb, Average bandwidth = 1 Kbps and Peak bandwidth = 4 Kbps.
Then we can say that Burst with rate of data 3 Kbps can remain for 1 second.

Congestion control in packet switching networks
Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



Open Loop Congestion Control
Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.
Policies adopted by open loop congestion control –

1. **Retransmission Policy :**It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy :**The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. **Discarding Policy :**A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. **Acknowledgment Policy :**Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

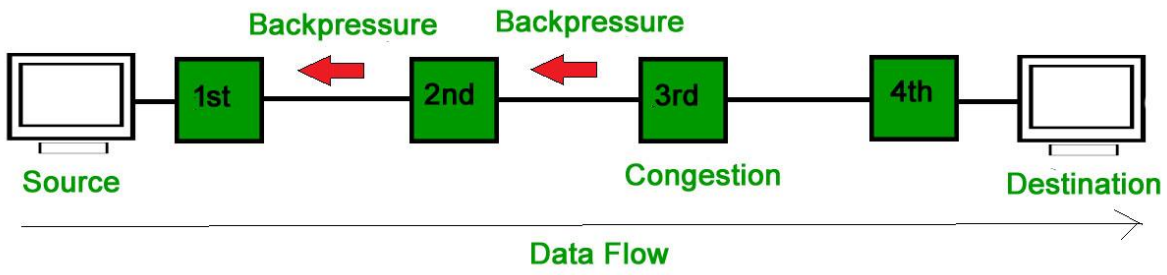
5. **Admission Policy :**In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

Closed Loop Congestion Control

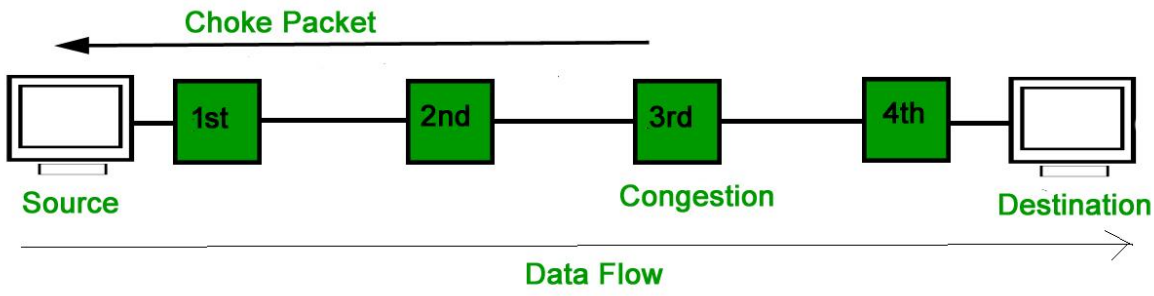
Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure : Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique : Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



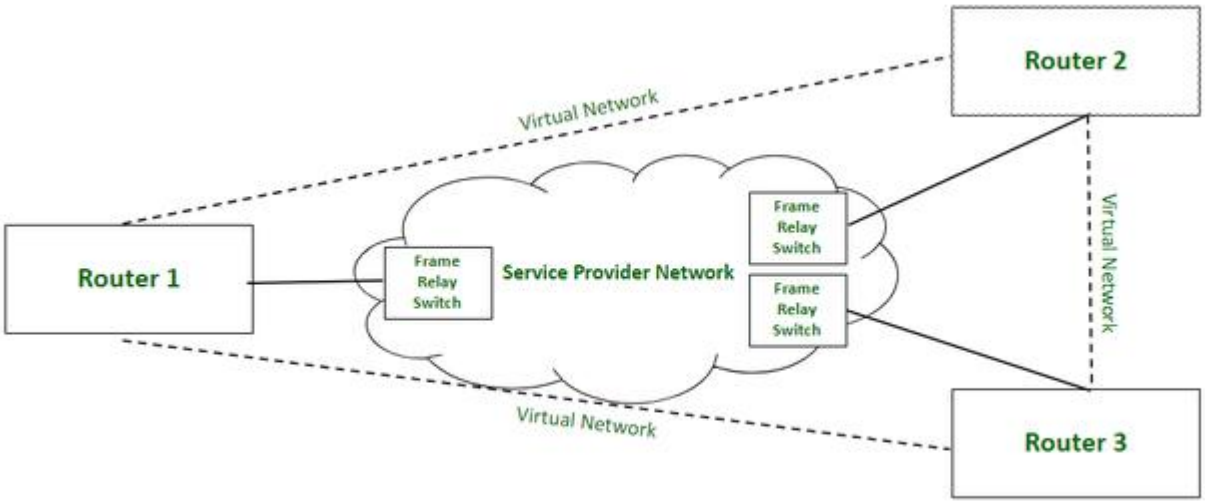
3. Implicit Signaling : In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling : In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique. Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling :** In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signaling :** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

FRAME RELAY CONGESTION CONTROL

Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation. Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.



FRAME RELAY NETWORK

Working:

Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network. It supports communication with multiple LANs over the shared physical links or private lines.

Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks. Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch. The access link is the private physical link used for communication with other LAN networks over WAN. The frame relay switch is responsible for terminating the access link and providing frame relay services.

For data transmission, LAN's router (or other border device linked with access link) sends the data packets over the access link. The packet sent by LAN is examined by a frame relay switch to get the Data Link Connection Identifier (DLCI) which indicates the destination of the packet. Frame relay switch already has the information about addresses of the LANs connected to the network hence it identifies the destination LAN by looking at DLCI of the data packet. DLCI basically identifies the virtual circuit (i.e. logical path between nodes that doesn't really exist) between source and destination network. It configures and transmits the packet to frame relay switch of destination LAN which in turn transfers the data packet to destination LAN by sending it over its respective access link. Hence, in this way, a LAN is connected with multiple other LANs by sharing a single physical link for data transmission.

Frame relay also deals with congestion within a network. Following methods are used to identify congestion within a network:

1. **Forward Explicit Congestion Network (FECN) –**FECN is a part of the frame header that is used to notify the destination about the congestion in the network. Whenever a frame experiences congestion while transmission, the frame relay switch of the destination network sets the FECN bit of the packet that allows the destination to identify that packet has experienced some congestion while transmission.

2. **Backward Explicit Congestion Network (BECN) –**BECN is a part of the frame header that is used to notify the source about the congestion in the network. Whenever a frame experiences congestion while transmission, the destination sends a frame back to the source with a set BECN bit that allows the source to identify that packet that was transmitted had experienced some congestion while reaching out to the destination. Once, source identifies congestion in the virtual circuit, it slows down to transmission to avoid network overhead.
3. **Discard Eligibility (DE) –**DE is a part of the frame header that is used to indicate the priority for discarding the packets. If the source is generating a huge amount of traffic on the certain virtual network then it can set DE bits of less significant packets to indicate the high priority for discarding the packets in case of network overhead. Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion within a network.

Types:

1. **Permanent Virtual Circuit (PVC) –**These are the permanent connections between frame relay nodes that exist for long durations. They are always available for communication even if they are not in use. These connections are static and do not change with time.
2. **Switched Virtual Circuit (SVC) –**These are the temporary connections between frame relay nodes that exist for the duration for which nodes are communicating with each other and are closed/ discarded after the communication. These connections are dynamically established as per the requirements.

Advantages:

1. High speed
2. Scalable
3. Reduced network congestion
4. Cost-efficient
5. Secured connection

Disadvantages:

1. Lacks error control mechanism
2. Delay in packet transfer
3. Less reliable

ATM TRAFFIC MANAGEMENT

Traffic Characteristics

Voice, video, and data traffic are differentiated by the following transmission characteristics:

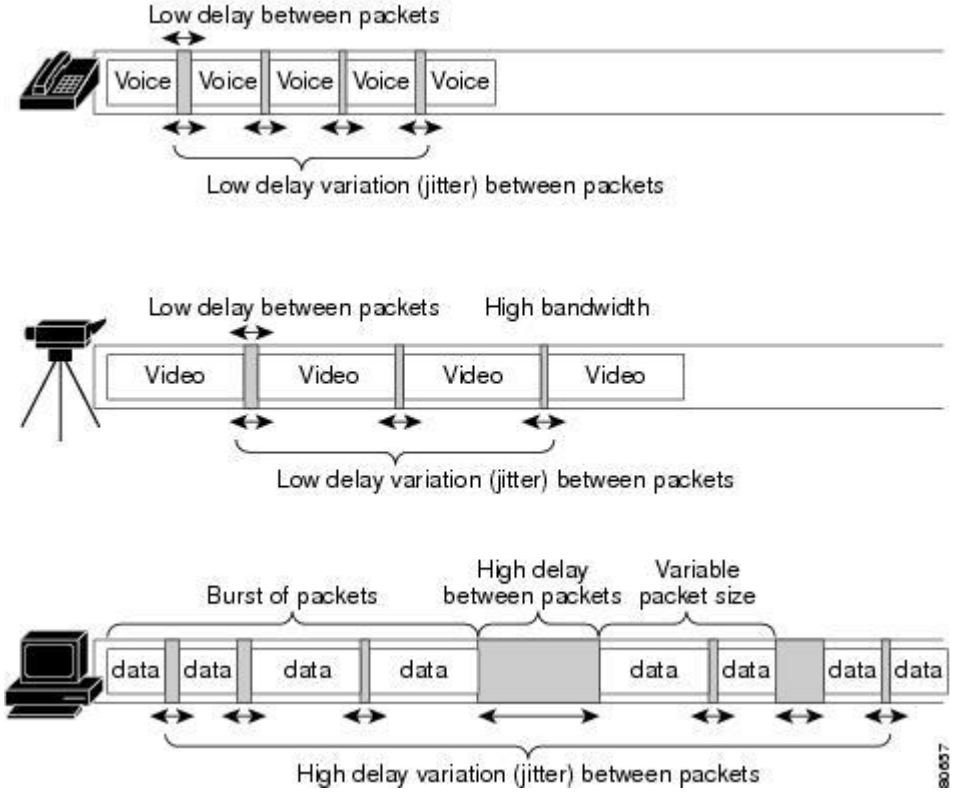
• Voice—Traffic flows with a regular pattern at a constant rate that is sensitive to delay and delay variation. When compression techniques are in use, voice traffic is more sensitive to error than uncompressed voice.

• Video—Real-time video traffic has similar transmission characteristics to voice traffic, but also requires high bandwidth. When compression techniques are in use, video traffic is more sensitive to error than uncompressed video.

• Data—Traffic flows with an irregular pattern that is often called *bursty* because of its variability in rate and amount of traffic. Data traffic is not sensitive to delay or delay variation, but it is sensitive to error.

Traffic management is vital to the performance and overall health of the ATM network. ATM uniquely satisfies the different transmission requirements of mixed traffic on a common network through its multiple service categories and QoS implementation.

Figure 1-1 Voice, Video, and Data Transmission Requirements



Traffic Contract

An ATM WAN is frequently a public network owned and managed by a service provider who supports multiple customers. These customers agree upon and pay for a certain level of bandwidth and performance from the service provider over that WAN. This agreement becomes the basis of the traffic contract, which defines the traffic parameters and the QoS that is negotiated for each virtual connection for that user on the network.

References to the traffic contract in an ATM network represent a couple of things. First, the traffic contract represents an actual service agreement between the user and the service provider for the expected network-level support. Second, the traffic contract refers to the specific traffic parameters and QoS values negotiated for an ATM virtual connection at call setup, which are implemented during data flow to support that service agreement.

The traffic contract also establishes the criteria for policing of ATM virtual connections on the network to ensure that violations of the agreed-upon service levels do not occur.

ATM Service Categories and Traffic Parameters

The ATM Forum Traffic Management specifications define several service categories to group traffic according to different transmission characteristics and performance needs. Each ATM service category is qualified by certain traffic parameters and QoS parameters that define the desired network performance for the permanent virtual circuit (PVC) or switched virtual circuit (SVC) on the ATM network.

The traffic parameters, sometimes called *descriptors*, are used to shape the flow of ATM cells. ATM service categories, and their corresponding traffic and QoS parameters, are the basis for differentiating services on the ATM network and for establishing the traffic contract for a particular connection.

Differences in Implementation of Traffic Parameters and QoS in PVCs and SVCs

All PVC and SVC traffic parameters and QoS parameters are established for the duration of a connection. The difference between PVCs and SVCs occurs in the implementation of these parameters.

On PVCs, traffic shaping parameters are based upon a manual configuration on both the edge device (router) and the switch. Therefore, no exchange of service-level information occurs between the edge device and the switch through signaling while a PVC connection is being established. Therefore, it is possible for configuration mismatches to occur between the router and the switch.

However, for SVCs, traffic parameters and QoS parameters are exchanged between the edge device and the switch through signaling. The edge device requests the required performance from the network, and the network responds with what it can provide. From there, the edge device can either accept or reject the connection. This is referred to as a *two-way handshake*.

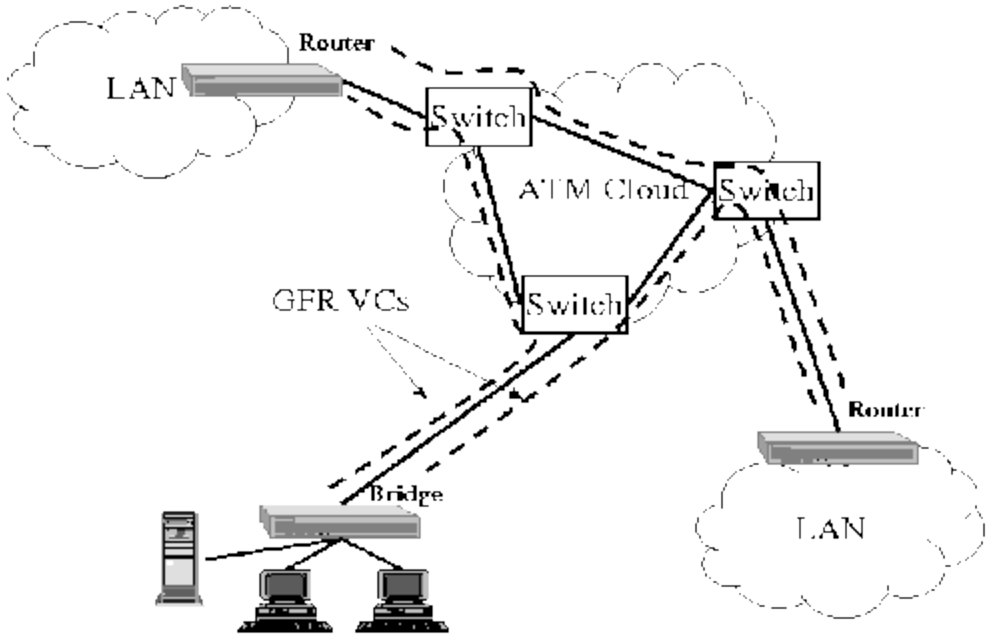
ATM Service Categories

The following ATM service categories are defined by the ATM Forum specifications and are supported on the Cisco 7200 series router to perform traffic shaping. The ATM service categories can be subdivided by their support for real-time or non-real-time applications.

ATM GFR

Guaranteed Frame Rate (GFR) has been recently proposed in the ATM Forum as an enhancement to the UBR service category. Guaranteed Frame Rate will provide a minimum rate guarantee to VCs at the frame level. The GFR service also allows for the fair usage of any extra network bandwidth. GFR requires minimum signaling and connection management functions, and depends on the network's ability to provide a minimum rate to each VC. GFR is likely to be used by applications that can neither specify the traffic parameters needed for a VBR VC, nor have cability for ABR (for rate based feedback control). Current internetworking applications fall into this category, and are not designed to run over QoS based networks. These applications could benefit from a minimum rate guarantee by the network, along with an opportunity to fairly use any additional bandwidth left over from higher priority connections. In the case of LANs connected by ATM backbones, network elements outside the ATM network could also benefit from GFR guarantees. For example, IP routers separated by an ATM network could use GFR VCs to exchange control messages. Figure 1illustrates such a case where the ATM cloud connects several LANs and routers. ATM end systems may also establish GFR VCs for connections that can benefit from a minimum throughput guarantee.

Figure 1: Use of GFR in ATM connected LANs



The original GFR proposals [11, 12] give the basic definition of the GFR service. GFR provides a minimum rate guarantee to the **frames**of a VC. The guarantee requires the specification of a maximum frame size (MFS) of the VC. If the user sends packets (or frames) smaller than the maximum frame size, at a rate less than the minimum cell rate (MCR), then all the packets are expected to be delivered by the network with minimum loss. If the user sends packets at a rate higher than the MCR, it should still receive at least the minimum rate. The minimum rate is guaranteed to the untagged frames of the connection. In addition, a connection sending in excess of the minimum rate should receive a fair share of any unused network capacity. The exact specification of the fair share has been left unspecified by the ATM Forum. Although the GFR specification is not yet finalized, the above discussion captures the essence of the service.

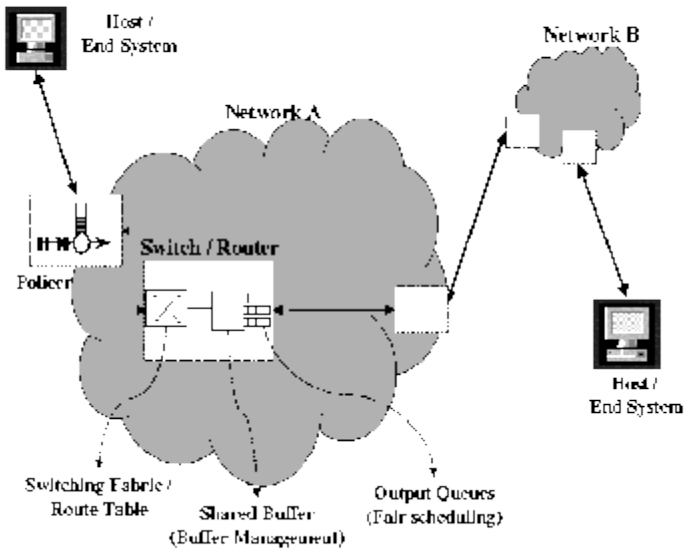
There are three basic design options that can be used by the *network*to provide the per-VC minimum rate guarantees for GFR - tagging, buffer management, and queueing:

1.

Tagging: *Network based tagging*(or policing) can be used as a means of marking non-conforming packets before they enter the network. This form of tagging is usually performed when the connection enters the network. Figure 2shows the role of network based tagging in providing a minimum rate service in a network. Network based tagging on a per-VC level requires some per-VC state information to be maintained by the network and increases the complexity of the network element. Tagging can isolate conforming and non-conforming traffic of each VC so that other rate enforcing mechanisms can use this information to schedule the conforming traffic in preference to

non-conforming traffic. In a more general sense, policing can be used to discard non-conforming packets, thus allowing only conforming packets to enter the network.

Figure 2: Network Architecture with tagging, buffer management and scheduling



2. **Buffer management:**Buffer management is typically performed by a network element (like a switch or a router) to control the number of packets entering its buffers. In a shared buffer environment, where multiple VCs share common buffer space, per-VC buffer management can control the buffer occupancies of individual VCs. Per-VC buffer management uses per-VC accounting to keep track of the buffer occupancies of each VC. Figure 2shows the role of buffer management in the connection path. Examples of per-VC buffer management schemes are Selective Drop and Fair Buffer Allocation [9]. Per-VC accounting introduces overhead, but without per-VC accounting it is difficult to control the buffer occupancies of individual VCs (unless non-conforming packets are dropped at the entrance to the network by the policer). Note that per-VC buffer management uses a single FIFO queue for all the VCs. This is different from per-VC queuing and scheduling discussed below.

3. **Scheduling:**Figure 2illustrates the position of scheduling in providing rate guarantees. While tagging and buffer management control the entry of packets into a network element, queuing strategies determine how packets are scheduled onto the next hop. FIFO queuing cannot isolate packets from various VCs at the egress of the queue. As a result, in a FIFO queue, packets are scheduled in the order in which they enter the buffer. Per-VC queuing, on the other hand, maintains a separate queue for each VC in the buffer. A scheduling mechanism can select between the queues at each scheduling time. However, scheduling adds the cost of per-VC queuing and the service discipline. For a simple service like GFR, this additional cost may be undesirable.