International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 07, Volume 4 (JULY 2017) www.irjcs.com

NETWORK CONGESTION CONTROL SYSTEM USING FRAME RELAY TECHNOLOGY

***Odii J. N.**
Department of Computer Science, Federal University of Technology, Owerri, Nigeria
jnodii@yahoo.com
Nwokoma F.O.
Department of Computer Science, Federal University of Technology, Owerri, Nigeria
adibefrancisca@yahoo.com
Onwuma T.U
Department of Computer Science, Federal University of Technology, Owerri, Nigeria
udora@yahoo.com
Eke J.I
Department of Computer Science, Federal University of Technology, Owerri, Nigeria
ekejoedike@gmail.com

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue07/JYCS10080**
DOI: 10.26562/IRJCS.2017.JYCS10080
Received: 05, June 2017
Final Correction: 20, June 2017
Final Accepted: 25, June 2017
Published: July 2017
Citation: **N., *O. J.; F.O., N.; T.U, O. & J.I, E. (2017), 'NETWORK CONGESTION CONTROL SYSTEM USING FRAME RELAY TECHNOLOGY', Master's thesis, Department of Computer Science, Federal University of Technology, Owerri, Nigeria.**
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

ABSTRACT- Frame-Relay is a technology that can be used to enhance the transmission of packets over a network. Over the years, the X.25 technology which has been widely used has led to several congestion problems and data loss during transmission of data through a network due to its inherent weak congestion control mechanism. The X.25 is a packet switched technology characterized with extensive protocol processing at the network nodes that causes delay and limits the available transfer speeds to 64 kbps, which is evidently insufficient for the end-users needs. It is therefore necessary to re-evaluate packet switching to meet the growing demands of the users. This research designs a network congestion control system using Frame Relay technology which uses DLCIs (Data Link Connection Identifiers), FECN (Forward Explicit Congestion Notification) and BECN (Backward Explicit Congestion Notification) to resolve the problem of queue management in the network, and modifies the mathematical model of the Queue control system in FECN thus eliminating congestion in the networks. While the Waterfall Methodology was deployed its design, the system was developed using Cisco Packet Tracer 6.0.1 for Windows and simulated using PHP, and XAMP. The Frame-Relay Technology is not only capable of reducing the prevalent congestion problems experienced in X.25 technology but also improves the low Speed of X.25 due to its incorporated efficient management of the queue in the switches during data transmissions.

Keywords: Packets, Congestion, Network, Protocol, Frame-relay.

I. INTRODUCTION

Frame Relay technology is a technology used to send packets from one area to another. Frame relay is a standardized interface that provides multiplexed access to bandwidth-on-demand backbone networks and delivers LAN-like performance over a wide area (Cavanagh, 1992). Since packets are sent over the network, there should be a means through which the number of packets being sent into the network is been resolved. When there are many packets in the same channel on the network, it can lead to congestion on the network.

And whenever there is congestion in the network, then there is possibility of loss of packets. In the recent years, there have been considerable developments in the area of telecommunications. These developments have led to the evolution of the concept of Integrated Services Digital Networks (ISDN). The main objective of these networks is to provide a range of voice and non-voice services over the same digital path via switched and non-switched connections. At the same time, the PC boom has led to the development of a decentralized system consisting of interacting local area networks, in which users exchange large amounts of data in the form of bursts. These changes in the communications pattern have led to an ever-growing need for higher transmission speeds.The traditional X.25 packet switching networks are however incapable of supporting this increase in user demand. (Anuradha,1993). Since the X.25 protocol was developed when most transmission technologies were analogue, it is characterized by extensive error recovery and flow control schemes. This extensive protocol processing at the network nodes causes delay and limits the available transfer speeds to 64 kbps, which is evidently insufficient for the end-user needs. It is therefore necessary to re-evaluate packet switching to meet the growing demands of the users. In addition, this re-evaluation is taking place with a digital world in mind. As the digital transmission facilities ensure a better quality of data transmission, there is no longer a need for extensive error correcting and flow controlling functions in the network node. These network protocols can therefore provide higher transmission speeds, and meet the demands of the users.

Moreover, with the prevalent congestion in X.25 technology in the transmission of packets across the Network, coupled with low Speed of X.25 due to inefficient management of the queue in the switches during data transmission, Frame relaying technology is still an option. Reason is that frame relay is one of the fast packet switching techniques with high oscillation of the Utility distribution. In frame relaying networks, error recovery and flow control takes place on an end-to-end basis. As a result, frame relay technology can offer up to 10 times the throughput of X.25. This paper therefore is set to design and implement a Network Congestion Control System using Frame-Relay Technology. And equally analyze Frame-Relay as a congestion control system in packet transmission from a sender to a receiver, Use of DLCIs to control the flow of packets across Networks, use of FECN and BECN to control the queue in the switches, suggest another strategy to help boost the speed of Frame-Relay in packet transmission and modifying the model used by Frame-Relay technology in bandwidth sharing among networks, in relation to the queue control mechanisms.

II. LITERATURE REVIEW

The frame relay (FR) technique is a packet-switched network technique used for the transmission of frames of varying length in place of the packet-switched network connections presently in use. The protocol (X.25) applied generally in the present packet-switched networks requires plenty of processing and the transmission equipment is expensive, as a result of which the speeds also remain low (Tero, et al. 1997). Frame relay is an adaptation of packet-switching technology developed for ISDN. The growing requirements of data users and mainly those resulting from LAN-to-LAN communications, coupled with two environmental changes have led to the evolution of frame relay technology. Firstly, devices that communicate via the network (Data Terminal Equipment) are now more intelligent and often connected to LANs with built-in error recovery to take account of errors occurring on the LAN.

Secondly, line quality has improved significantly, as digital transmission facilities have replaced analogue lines. The growing incidence of fiber reduces the transmission errors still further to a negligible level. As the high quality and speed of the modern transmission links reduces the need for error control on a per-link basis, frames are simply forwarded through the frame relay network without error correction. Errors or congestion problems will result in frames being discarded and recovery is the responsibility of the end user systems. By taking responsibility for some functions away from the network, the bandwidth and processing overheads in frame relay networks is less than that in conventional X.25 networks, and a much faster packet-switching facility is provided. The use of Frame-relay by companies was the beginning of a massive shift of communication paradigm from Local Area Networks (LAN) to networks that can cover large geographical areas. Businesses, local and state governments, and individual consumers are all trying to use Frame-Relay with congestion control to their communication benefit.

A. Packet Switched Services.

In packet-switched technology, blocks of data are individually transmitted from a source to a destination across a network. The packets from multiple users share the same transmission path and distribution facilities. They are stored and forwarded at each node along a path, sharing buffer and link transmission resources with all other packets being transmitted across a given link on the path (Anuradha,1993).Wide Area Network (WAN) technologies that rely on public networks via packet-switching (a method of encoding data into small, uniquely identified chunks known as packets) have been increasingly popular over the past decades. Two of the most important packet-based technologies are frame relay and asynchronous transfer mode (ATM).Frame relay is older among the two, and came into general use in the early 1990s. ATM services, which were introduced commercially in the mid-1990s, are based on similar principles.

ATM is a transfer mechanism which uses fixed sized packets called cells and statistical (label) multiplexing which allows the cells to be assigned on demand. Cells are identified as belonging to a particular logical connection by the Virtual Channel Identifier (VCI) that is carried as a label in the header of every cell. ATM is a connection oriented technique and provides a common lower layer transport mechanism for all services (Abensour, et al. 1996).Many have touted ATM as a break-through technology, but as of the late 1990s it had only a modest impact on the WAN market. ATM employs a concept called cell relay to transmit data. Cells are uniformly sized, small packets of data; in the case of ATM, just 53 bytes each, including a 5-byte header. By contrast, a frame relay packet may range up to several thousand bytes. As with frame relay, ATM transfers data over a defined virtual path rather than allowing packets to follow any number of paths to their destinations, as occurs in TCP/IP protocols used in Internet applications. This highly stable connection lends itself to video and other applications that require a steady, predictable flow of data. The drawbacks to this certainty are that the constant level of service may be low compared to other options, and ATM may not be well equipped to manage short-term spikes in demand for network resources.

B. Congestion

An important issue in a packet-switched network is congestion. Congestion in a network may occur if the load on the network -the number of packets sent to the network- is greater than the capacity of the network -the number of packets a network can handle. Overload or congestion control is one of the key mechanisms to accommodate the increasingly diverse range of services and types of traffic in the Internet. Congestion control relates to the general problem of traffic management for packet-switched networks (Ma, et al. 2008).Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. The question then is "why is there congestion on a network?" Congestion happens in any system that involves waiting. For example, congestion happens on a freeway because any abnormality in the flow, such as an accident during rush hour, creates blockage.

Congestion in a network or inter-network occurs because routers and switches have Queues-buffers that hold the packets before and after processing. A router, for example, has an input queue and an output queue for each interface. When a packet arrives at the incoming interface, it undergoes three steps before departing; the steps are as outlined below:

(a). The packet is put at the end of the input queue while waiting to be checked.
(b). The processing module of the router removes the packet from the input queue once it reaches the front of the queue and uses its routing table and the destination address to find the route.

3. The packet is put in the appropriate output queue and waits for its turn to be sent, (http://www.idconline.com). It is important to note that , if firstly the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer. Second, if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.

C. Network Performance

Congestion control involves two factors that measure the performance of a network: *delay* and *throughput.* Figure 2.1 shows these two performance measures as function of load.

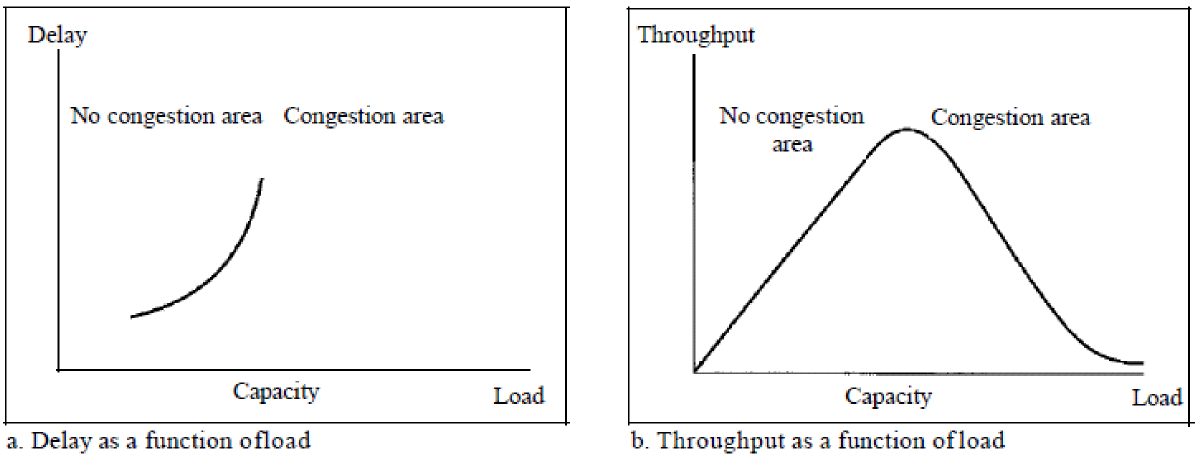

Fig 2.1: Packet Delay and Throughput as Functions of Load.

Delay versus Load

Notice that 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 waiting time in the queues (for all routers in the path) to the total delay. Note that the delay becomes infinite when the load is greater than the capacity. If this is not obvious, consider the size of the queues when almost no packet reaches the destination, or reaches the destination with infinite delay; the queues become longer and longer. Delay has a negative effect on the load and consequently the congestion. When a packet is delayed, the source, not receiving the acknowledgment, retransmits the packet, which makes the delay, and the congestion, worse.

Throughput versus Load

Throughput in a network can be defined as the number of packets passing through the network in a unit of time. Notice that when the load is below the capacity of the network, the throughput increases proportionally with the *load.* It is expected that the throughput remains 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 packet; 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.

D. Congestion Control

Congestion control refers to techniques and mechanisms that can prevent congestion, either before it happens, or remove congestion, after it has happened. In general, congestion control mechanisms is divided into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) (http://mvn.edu.in/lms/mod/book/view.php?id=72)

Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.

(i) Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion. For example, the retransmission policy used by TCP (explained later) is designed to prevent or alleviate congestion.

(ii) Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent, although some may have arrived safely at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

(iii) Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only *N* packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

(iv) Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

(v) Admission Policy

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

E. Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

(i) Backpressure

The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is coming. Figure 2.2 shows the idea of backpressure.

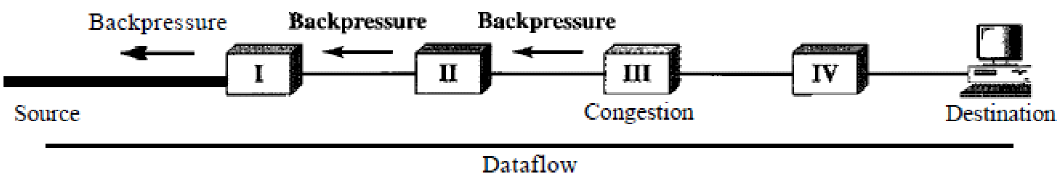

Figure 2.2: Backpressure method for alleviating congestion

Source: http://mvn.edu.in/lms/mod/book/view.php?id=72

Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion. If so, node I informs the source of data to slow down. This, in time, alleviates the congestion. Note that the *pressure* on node III is moved backward to the source to remove the congestion. None of the virtual-circuit networks we studied in this book use backpressure. It was however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

(ii) Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned. We have seen an example of this type of control in ICMP. When a router in the Internet is overwhelmed with IP datagram, it may discard some of them; but it informs the source host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action. Figure 2.3 shows the idea of a choke packet.

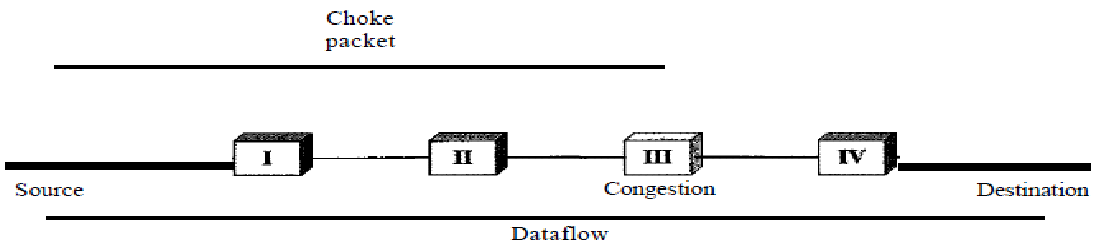

Figure 2.3: Choke packet

Source: http://mvn.edu.in/lms/mod/book/view.php?id=72

(iii) Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down. We will see this type of signaling when we discuss TCP congestion control later in the chapter.

(iv) Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data.Explicit signaling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction. Backward Signaling A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets. Forward Signaling A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

III. THE FRAME RELAY TECHNOLOGY

The goal of frame relay technology is to reduce the scattered Nature of the Utility distribution. This will thus help in increase in the Throughput of the Network. When the Service rate is made inversely proportional to the Load factor there is a reduction in the utility of the sources. Thus the utility distribution is more compact. This is how the E-FECN works. To modify this, it will be more productive if we divide the Load Factor, (Not the one used in E-FECN but the one used in FECN), by the queue functions power of maximum number of packets. $Rs(i+1) = Rs(i)/(L/Q^{Qm})$ $L = Ra/C$

A. Congestion Control Using Frame Relay

Congestion in a Frame Relay network decreases throughput and increases delay. A high throughput and low delay are the main goals of the Frame Relay protocol. Frame Relay does not have flow control. In addition, Frame Relay allows the user to transmit busty data. This means that a Frame Relay network has the potential to be really congested with traffic, thus requiring congestion control.

i) Congestion Avoidance

For congestion avoidance, the Frame Relay protocol uses 2 bits in the frame to explicitly warn the source and the destination of the presence of congestion. The Backward Explicit Congestion Notification (BECN) bit warns the sender of congestion in the network. One might ask how this is accomplished since the frames are traveling away from the sender.

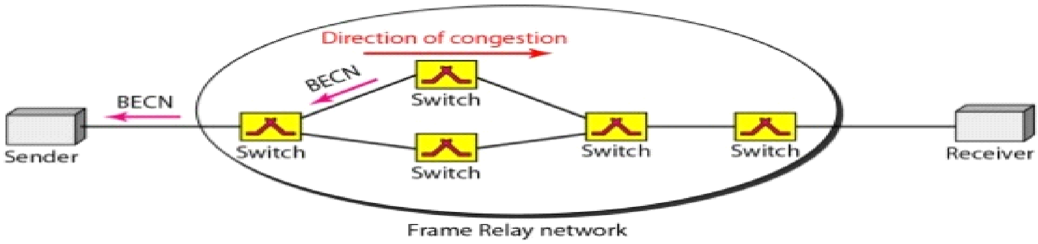

Figure 3.1 The Use of BECN

Source:http://image.slidesharecdn.com/24congestioncontrolandqualityofservice-160210170745/95/24-congestion-controlandqualityofservice-20-638.jpg?cb=1455124099

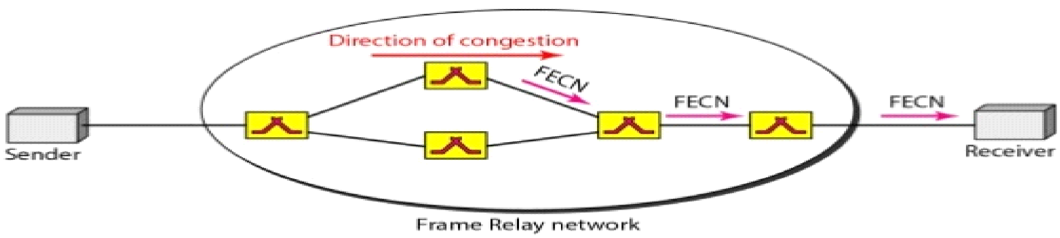

Figure 3.2: The Use of FECN

Source:http://image.slidesharecdn.com/24congestioncontrolandqualityofservice-160210170745/95/24-congestion-controlandqualityofservice-21-638.jpg?cb=1455124099

In fact, there are two methods: The switch can use response frames from the receiver (full-duplex mode), or the switch can use a predefined connection (DLCI =1023) to send special frames for this specific purpose. The sender can respond to this warning by simply reducing the data rate. Figure 3.2 below shows the use of BECN. The Forward Explicit Congestion Notification (FECN) bit is used to warn the receiver of congestion in the network. It might appear that the receiver cannot do anything to relieve the congestion. However, the Frame Relay protocol assumes that the sender and receiver are communicating with each other and are using some type of flow control at a higher level. For example, if there is an acknowledgment mechanism at this higher level, the receiver can delay the acknowledgment, thus forcing the sender to slow down. Figure 3.2 shows the use of BECN.

International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 07, Volume 4 (JULY 2017) www.irjcs.com

When two endpoints are communicating using a Frame Relay network, four situations may occur with regard to congestion. Figure 3.3 shows these four situations and the values of FECN and BECN.

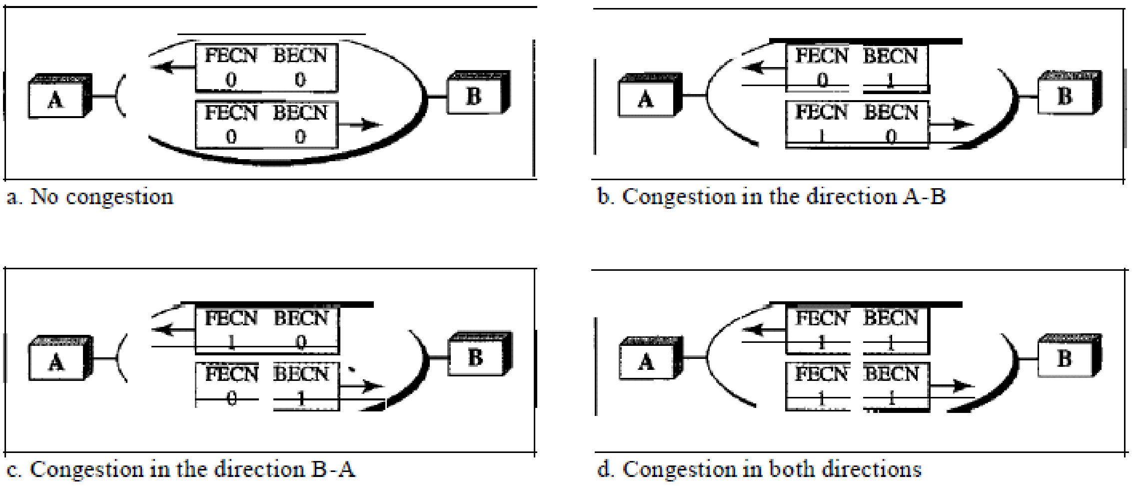

Figure 3.3 Four Situations and the Values of FECN and BECN.

SOURCE: https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch24.pdf

IV. IMPLEMENTATION OF FRAME RELAY ARCHITECTURE.

In Frame Relay implementation, the connection between a DTE (router) device and a DCE (Frame Relay switch) device which consists of both a physical layer component and a link layer component works as follows:

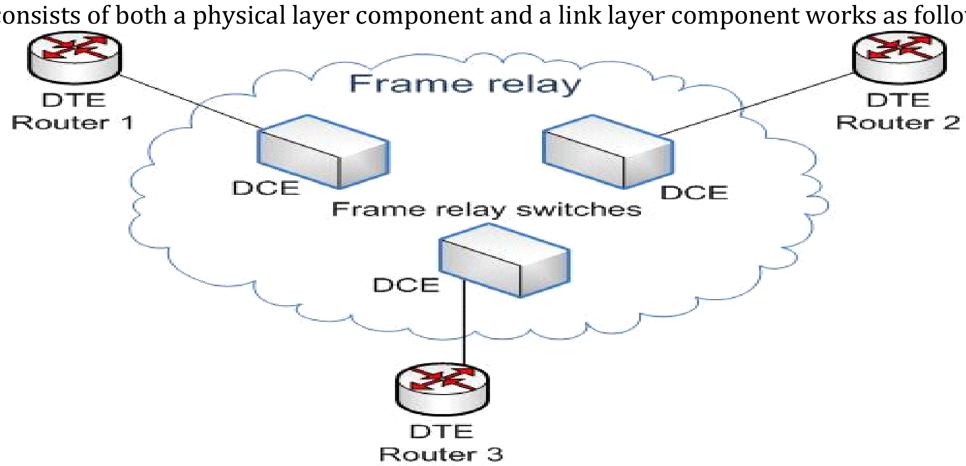

Figure 4.1: FRAME RELAY ARCHITECTURE

Source:https://upload.wikimedia.org/wikipedia/commons/thumb/2/2e/Frame_relay.jpg/350px-Frame_relay.jpg

a). The physical component defines the mechanical and electrical specifications the connection between the devices.

b).The link layer component defines the protocol that establishes the connection between the DTE device, such as a router, and the DCE device, such as a switch.

When interconnection between LANs are implemented using frame relay, the LAN Gateway router (DTE) is connected to the Frame Relay switch (DCE) through a serial connection such as a T1/E1 leased line, at the nearest point-of-presence (POP) or WAN edge. Network switches move frames from one DTE across the network and deliver frames to other DTEs via DCEs. Other network computing equipment that is not on a LAN may also send data across a Frame Relay network by using a Frame Relay access device (FRAD) as the DTE. The FRAD is sometimes referred to as a Frame Relay assembler/dissembler and is a dedicated appliance or a router that is configured to support Frame Relay. It is located on the customer's premises and connects to a switch port on the service provider's network. In turn, the service provider interconnects the Frame Relay switches.

In a nutshell, the frame relay frame work can be summarized as follows:

1. The DTE (router) sends frames to the DCE (Frame relay Switches) on the WAN edge.
2. The frames move from switch to switch across the WAN to the destination DCE (frame relay switch) on the WAN edge.
3. The destination DCE delivers the frames to the destination DTE.

Formerly, the congestion control in the frame relay technology have been enhanced which brought about E-FECN (Enhanced forward Explicit Congestion Notification), from the original technology FECN. This brought about a drastic improvement in the Queue control functionality of the frame relay. This was done by the enhancement of Queue-Control, Exponential averaging, Limited Rate Increase, Variable Capacity Adjustment; Time based Sampling at the Source. In the enhancement of FECN, it was shown that the Load factor is inversely proportional to the queue function. Also the Hyperbolic function is better for calculation of the queue function. The bandwidth allocation is inversely proportional to the Load factor.

Hence, we calculate the queue length as:

$$Q= (b\times MaxQ)/(((b-1)\times q)+MaxQ) \quad \text{(if } q<=MaxQ)$$

or

$$Q= \max(c,(a\times MaxQ)/(((a-1)\times q)+MaxQ)) \quad \text{(if } q >MaxQ)$$

For : $a=1.1; b=1.002; c=0.1$

And $q = Ra^2/(Rs\times(Rs-Ra))$

$R = C/N$

$Rs(i+1) = Rs(i)/L$

$U = Ra/Rs$

$L = Ra/L$

$Ra = Nm/Dl$

Where;

S= Initial Service Rate ; C= Link Capacity; N= Number of Sender; Ra= Arrival Rate = Ra; Np= Number of Packets in the system; Dl = Average delay per Packet ; L= Load Factor; Q= Queue Function; Qm= Maximum number of packets in the queue; Rs= Service Rate; q= Queue length; and U= Utility.

V. THE SIGNIFICANCE OF FRAME RELAY TECHNOLOGY

A. Low Delay: Among the benefits gained by using frame relay technology is the very low delay through a frame relay switching node. The overall delay of the network itself is also reduced because of high speed access lines are used and because of full bandwidth of the backbone lines is available to the data as it traverses the network. Combining these two advantages, users are able to reduce waiting time for network to complete a transaction, thus productivity is increased.

B. Protocol Transparency: Another advantage of frame relay is its protocol transparency above layer two. Frame relay allows switching of X.25, SNA, TCP/IP, or any other HDLC-like protocols with equal ease.

C. Data Switching: Another major benefit of frame relay is the performance of data switching, the network achieves connectivity of endpoints. In other words, it can communicate with any other endpoint so long as there is a pre-established connection identifier. Even better, this connectivity is achieved without any penalty whatsoever in terms of numbers of ports, number of access lines or capacity required on the backbone trunks. Frame relay can co-exist with ISDN, but does not require ISDN. It will be compatible with future implementations of ISDN such as B-ISDN. In summary, frame relay effectively meets the modern requirements for a high-speed, packet-mode network.

D. Congestion Control: With the right congestion control mechanism the problem of congestion during Network growth is eliminated.

VI. SUGGESTION FOR FURTHER WORK

The system can be enhanced so that users can appreciate Frame-Relay better. Frame-Relay should be combined with ATM (Asynchronous Transfer Mode) so as to combine the benefits of circuit switching with those of packet switching. It provides scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (GBps).

VII. CONCLUSION

Although frame relay is a standardized interface that provides multiplexed access to bandwidth-on-demand backbone networks and delivers LAN like performance over a wide area, frame relay networks are equally vulnerable to congestion. Therefore flow and congestion control strategies have been essentially explored to prevent the degradation of the network performance. The use of congestion notification bits also to initiate congestion avoidance procedures have been specified in the frame relay standards.

REFERENCE

1. Abensour, Daniel S. , Fox, Jon E., Joshi, Mahendra J., Lai, Fuyung Sy, Kian-Bon K.(1996):
2. System and method for providing ATM support for frame relay DTEs with a terminal adapter, google Patents.
3. Anuradha S. (1993); Flow and Congestion Control in Frame relay Networks. Dublin City University doras.dcu.ie>anura_sahgal_201307….
4. Cavanagh, J. P. (1992). "Applying the frame relay interface to private networks." IEEE - Xplore : 48-54. ieeexplore.ieee.org

5. Tero, P., Jorma, M., Jorma H., Esa S., Heikki K., Jukka M., Kari R. O. (1997). Method for congestion management in a frame relay network and a node in a frame relay network, Google Patents.
6. Kajsa L. (1992) "Frame Relay- for faster and more efficient data communications"; Ericsson review no. 1-2
7. Ma, Jian, Peng, Fei, Wu, Jing. (2008). Congestion control method for a packet-switched network, Google Patents.
8. "http://searchenterprisewan.techtarget.com/definition/framerelay"SearchEnterpriseWANHYPERLINK. Retrieved 9 April 2012.
9. (http://www.idconline.com/technicalreferences/pdfs/datacommunications/CongestionControl.pdf 1:04PM 17/10/2016).
10. http://mvn.edu.in/lms/pluginfile.php/123/mod_book/chapter/21/Q2.png
11. http://mvn.edu.in/lms/mod/book/view.php?id=72
12. https://upload.wikimedia.org/wikipedia/commons/thumb/2/2e/Frame_relay.jpg/350px-Frame_relay.jpg
13. https://www.cpe.ku.ac.th/~plw/dccn/presentation/ch24.pdf

