# Designing of Wide Area Network with the use of Frame Relay Concept in Real Time Environment: a Proposal

[1]Mohammad Zunnun Khan, [2]Prof. (Dr.) Mohd. Rizwan Beg [3]Mohd. Shahid Husain

[1]*zunnunkhan@gmail.com*

[1, 2, 3] *Integral University, Lucknow*

***Abstract*— These days inter-domain routing protocol, i.e., BGP (Border Gateway Protocol), is getting complicated day by day due to policy mis-configuration by individual autonomous systems. Existing configuration analysis techniques are either manual or tedious, or do not scale beyond a small number of nodes due to the state explosion problem. To aid the diagnosis of mis-configurations in real-world large BGP systems, this paper presents BGP based on Packet Switching Technology and Inter-VLAN where as packet switching technology is WAN technology. Inter-VLAN is a technology to communicate between two or more VLAN's. A company can send or receive any type of data, either text image, video etc. Another important part of network is security. This network would make use of following protocol for security purpose such as PAP, CHAP, ACL, and NAT. The key idea is that, all transmissions are broken into units called packets, each of which contains addressing information that identifies both the source and destination nodes. These packets are then routed through various intermediaries, known as *Packet Switching Exchanges* (*PSE*s), until they reach their destination.**

**And there are two parameters associated with a Frame Relay connection are; Committed Information Rate (CIR), Peak Information Rate (PIR) Cisco configuration guidelines, as well as arbitrary user-defined networks. This method improves the applicability, efficiency, and benefits of the network deployment, it also introduces an infrastructure that enables networking researchers to interact with advanced formal method tool.**

***Index Terms*— BGP, network simulation, Frame Relay, VLAN, X.25**

*****

## I. INTRODUCTION

The Internet today runs on a complex routing protocol called the Border Gateway Protocol or BGP for short. BGP enables autonomous systems worldwide to achieve global connectivity [1], subject to each system's local policy (what paths are allowed and the route preference used to select best paths). The convergence behavior of the global Internet depends on how each ISP configures its policy. Prior work has shown that policy mis-configurations can lead to route oscillation and slow convergence [2]. While our understanding of BGP safety has improved dramatically in the past decade, there is a lack of automated tools that can aid in the safety analysis process.

In this demonstration, we will show a wide area network for system by which system can communicate within its branch. We use Packet Switching Technology and Inter-VLAN where as packet switching technology is WAN technology. Inter-VLAN is a technology to communicate between two or more VLANs. A system can send or receive any type of data. Another important part of network is security. In this network would make use of following protocol for security purpose such as PAP, CHAP, ACL, and NAT.

Procedure for Paper Submission

### *A Packet Switching Technology*

Packet switching, although it is also involved in routing data within and between LANs such as Ethernet and Token Ring, is also the backbone of WAN routing [3]. It's not the highway, on which the data packets travel, but it is the dispatching system and to some extent the cargo containers that carry the data from place to place. In packet switching, all transmissions are broken into units called packets, each of which contains addressing information that identifies both the source and destination nodes, and routed through various intermediaries, known as Packet Switching Exchanges, until they reach their destination. At each stop along the way, the intermediary inspects the packet's destination address, consults a routing table, and forwards the packet at the highest possible speed to the next link in the chain leading to the recipient.

This is a WAN switching method that allows you to share bandwidth with other companies to save money. Packet switching can be thought of as a network that's designed to look like a leased line, yet charges some cost more like circuit switching. Packet switching will work well if your data transfers are bursty in nature. Frame Relay and X.25 are packet-switching technologies. Speeds can range from 56Kbps to T3 (45Mbps). [5]

### *B. Frame Relay*

Frame Relay is a high performance, low delay product that supplies cost effective LAN, WAN, Internet and Intranet interconnections. It is most suitable for sending variably

sized bursts of data that require peak speeds.

It uses the telecommunications provider's packet-switching infrastructure to move data. Frame Relay can provide speeds from 56kbps DS0 up to 43Mbps DS3 connections depending on the capability of the service provider's network.

Frame Relay is a high-speed communications technology that is used throughout the world to connect LAN, Systems Network Architecture (SNA), Internet, voice and other end-user network applications.

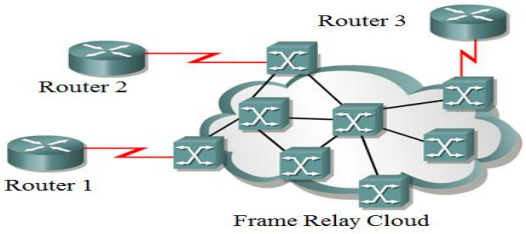


*Fig 1 Frame Relay Cloud.*

It sends information over a WAN by dividing data into frames or packets, each of which has an address that the network uses to determine the destination of each frame. To reach the destination these frames travel through a series of switches within the frame relay network. Frame Relay is a statistically multiplexed protocol based on data network standards developed specifically to handle high speed applications with "bursty" traffic, such as LANs, host computers and high performance workstations. The three main components of the Frame Relay service are:

1) Endpoints (PCs, servers, host computers).

2) Access equipment (routers, hosts).

3) Network devices (switches, multiplexers, network routers).

Although a Frame Relay connection is effectively a point to point connection. a frame relay network will often be depicted as a network cloud, because it does not provide a single physical connection between one endpoint and another. Instead a logical path is defined within the network. This logical path is called a permanent virtual circuit (PVC) [4]. Multiple point to point PVC's can be meshed to create point to multi-point access.

There are two parameters associated with a Frame Relay connection are:-

1) Committed Information Rate (CIR) – the minimum amount of bandwidth that the network ensures will always be available for the specific Permanent Virtual Circuit (PVC).

2) Peak Information Rate (PIR) – the maximum amount of bandwidth available for this specific PVC. Frame Relay offers a wide range of PVC options to meet end-user requirements. End-users can choose their desired PIR and then can select from one of 4 CIR Bands, ranging from25% to 100%.1.3 Inter-VLAN Routing

We define inter-VLAN routing as a process of forwarding network traffic from one VLAN to another VLAN using a router. To allow devices connected to the various VLANs to communicate with each other, you need to connect a router. As we've learned that each VLAN is a unique broadcast domain, so, computers on separate VLANs are, by default, not able to communicate. There is a way to permit these computers to communicate; it is called inter-VLAN routing [4].

One of the ways of the ways to carry out inter-VLAN routing is by connecting a router to the switch infrastructure. VLANs are associated with unique IP subnets on the network. This subnet configuration enables the routing process in a multi-VLAN environment. When using a router to facilitate inter-VLAN routing, the router interfaces can be connected to separate VLANs. Devices on those VLANs communicate with each other via the router. [6]

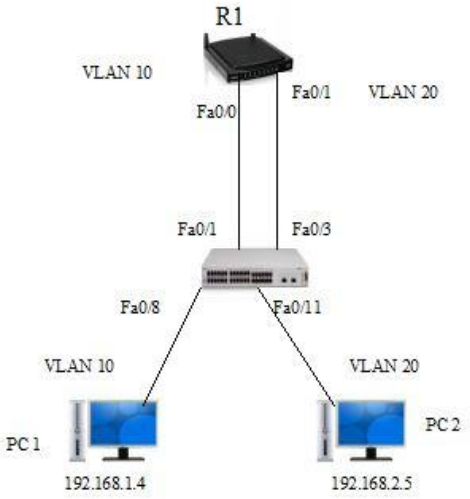


*Fig 2 Router and PC Communitcation.*

Traffic from PC1 VLAN 10 is routed through router R1 to reach PC3 on VLAN 20.

PC1 and PC2 has a separate interface configured for each of the VLANs.

Traffic from PC1 VLAN 10 is routed through router R1 to reach PC3 on VLAN 20.PC1 and PC2 has a separate interface configured for each of the VLANs. Router R1 has a separate interface configured for each of the VLANs.

## II Related Work

The last few years there has been a considerable work on BGP simulation research. The BGP model by Premore in the SSFnet simulator was the first detailed simulation model of BGP and is currently the most widely used BGP simulator. It supports most important BGP features and extensions. The main limitation of SSFnet is that it exhibits considerable memory demand, thereby preventing simulations larger than a few hundred of BGP routers. Among these effors, the C-BGP [11] simulator and the work by Hao and Koppol [12] emphasize on large-scale BGP simulations. C-BGP is a BGP decision process simulator that, can read CISCO-like configuration-less and can simulate large-scale topologies.

Nevertheless, it only implements the BGP decision process, ignoring several details of the protocol, namely timers and BGP messages.

The recent work by Hao and Koppol [12] addresses the challenge of large-scale

BGP simulations by ignoring the protocol stack bellow the application layer. Their simulator can perform large-scale experiments. Nevertheless, the relevant paper [12] does not discuss sufficiently the features of the simulator so as to develop a comprehensive picture of the work.

### A. Leased Line

A leased line is a service contract between a provider and a customer, whereby the provider agrees to deliver a symmetric telecommunications line connecting two or more locations in exchange for a monthly rent (hence the term lease). It is sometimes known as a 'Private Circuit' or 'Data Line' in the UK or as CDN (Circuito Diretto Numerico) in Italy [14]. Unlike traditional PSTN lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services. Some are ringdown services, and some connect two PBXes.

### B. Circuit Switching Technology

Circuit switching involves creating a direct physical connection between sender and receiver, a connection that lasts as long as the two parties need to communicate. In order for this to happen, of course, the connection must be set up before any communication can occur. Once the connection is made, however, the sender and receiver can count on "owning" the bandwidth allotted to them for as long as they remain connected.

Although both the sender and receiver must abide by the same data transfer speed, circuit switching does allow for a fixed (and rapid) rate of transmission. The primary drawback to circuit switching is the fact that any unused bandwidth remains exactly that: unused. Because the connection is reserved only for the two communicating parties, that unused bandwidth cannot be "borrowed" for any other transmission.

### C. ISDN

Integrated Services Digital Network (ISDN) is a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book. [14] Prior to ISDN, the phone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI) and Broadband ISDN (B-ISDN).

### D. X.25 packet-switching network.

Originating in the 1970s, X.25 is a connection-oriented, packet-switching protocol, originally based on the use of ordinary analog telephone lines that has remained a standard in networking for about twenty years. Computers on an X.25 network carry on full-duplex communication, which begins when one computer contacts the other and the called computer responds by accepting the call [15].

Although X.25 is a packet-switching protocol, its concern is not with the way packets are routed from switch to switch between networks, but with defining the means by which sending and receiving computers (known as DTEs) interface with the communications devices (DCEs) through which the transmissions actually flow. X.25 has no control over the actual path taken by the packets making up any particular transmission, and as a result the packets exchanged between X.25 networks are often shown as entering a cloud at the beginning of the route and exiting the cloud at the end.

## III Proposed Frame Work

The representation is based on CISCO, all the router, switch are used which is made by CISCO [14], and all the protocol which is used to configure the router, switch are used to implement WAN and some protocol are used to provide security. So, first step is to know the branches of company. We first prepare Local Area Network (LAN) at different location of branches, and then we connect all the different LAN. As the LAN is establish at different branches, we use Wide Area Network (WAN) technology such as Frame Relay to connect different branches of company. Hence our proposal will show entire network of company and its branches, would implement cost effective and reliable network as possible. Another important part of network is security [13]. This network would make use of following protocol for security purpose such as PAP, CHAP, ACL, and NAT. Hence, company can send or receive any type of data text, image, video or other. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as EIGRP to communicate with each other and configure the best route between any two hosts

**A. Virtual LAN** A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. To physically replicate the functions of a VLAN, it would be necessary to install a separate, parallel collection of network cables and switches or hubs which are kept separate from the primary network. However unlike a physically separate network, VLANs must share bandwidth. VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and

traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain. We are focusing only one Cisco switching and routing product lines running Cisco IOS.

VLAN ID - The VLAN ID is a unique value you assign to each VLAN on a single device. With a Cisco routing or switching device running IOS, your range is from 1-4096. When you define a VLAN you usually use the syntax "vlan x" where x is the number you would like to assign to the VLAN ID. VLAN 1 is reserved as an administrative VLAN. If VLAN technologies are enabled, all ports are a member of VLAN 1 by default.

VLAN Name - The VLAN name is an text based name you use to identify your VLAN, perhaps to help technical staff in understanding its function. The string you use can be between 1 and 32 characters in length.

Private VLAN - You also define if the VLAN is to be a private vlan in the VLAN definition, and what other VLAN might be associated with it in the definition section. When you configure a Cisco VLAN as a private-vlan, this means that ports that are members of the VLAN cannot communicate directly with each other by default. Normally all ports which are members of a VLAN can communicate directly with each other just as they would be able to would they have been a member of a standard network segment. Private vlans are created to enhance the security on a network where hosts coexisting on the network cannot or should not trust each other. This is a common practice to use on web farms or in other high risk environments where communication between hosts on the same subnet are not necessary. Check your Cisco documentation if you have questions about how to configure and deploy private VLANs.

VLAN modes - in Cisco IOS, there are only two modes an interface can operate in, "mode access" and "mode trunk". Access mode is for end devices or devices that will not require multiple VLANs. Trunk mode is used for passing multiple VLANs to other network devices, or for end devices that need to have membership to multiple VLANs at once. If you are wondering what mode to use, the mode is probably "mode access".

## IV. Conclusions and Future Work

In this work we develop BGP: a scalable and detailed BGP simulator that is built on top of high quality software in network simulation (ns-2), here Implementing WAN using Packet Switching Technology and Inter-VLAN is flexible enough to meet the requirements of the Organization. This project will help in enhancing the knowledge and alleviating the skills in the field of networking by adding up hands on experience in the same for anyone. This project not only increases the efficiency of the working but also attains maximum user requirement by providing them suitable service.

The most important aspect of any organization is how quickly and accurately one can get up-to-date information from one place.

As there is rapid growth in networking. Hence, there will be enhancement in this project by adding ATM (Asynchronous Transfer Mode). It encodes data into small, fixed-sized cells. This differs from networks such as the Internet or Ethernet LANs that use variable sized packets or frames. ATM provides data link layer services that run over OSI Layer 1 physical links. ATM has functional similarity with both circuit switched networking and small packet switched networking.

Evaluating the future performance of the interdomain infrastructure is a problem in which simulation is essential. With the current growth rates, Internet will have more than 34,000 ASs by 2012. It is unknown how BGP performance and problems will be shaped by the increased complexity and scale. Large-scale BGP simulations are necessary to shed light on the scalability limits of BGP.

Finally, a systematic framework for BGP network control, configuration testing and problem diagnosis is another application of network simulation. We envision a simulation interface that replicates a real network, providing practical tools to check topological or configuration changes and to diagnose unforeseen problems.

## REFERENCES

[1] C. Labovitz, A. Ahuja, A. Bose, F. Jahanian, Delayed Internet routing convergence, in: Proceedings of ACM SIGCOMM, 2000, pp. 175.187.

[2] C. Labovitz, A. Ahuja, R.Wattenhofer, S. Venkatachary, The impact of Internet policy and topology on delayed routing convergence, in: Proceedings of INFOCOM, 2001, pp. 537.546.

[3] P. Baran et al., "On distributed communications, vols. I-XI. " RAND Corporation Research Documents.
Aug. 1964.

[4]. T. Marill and L. G. Roberts, "Toward a cooperative network of time-shared computers," Proc. FJCC pp. 425-431, 1966.

[5]. D. W. Davies, K. A. Bartlett, R. A. Scantlebury, and P. T. Wilkinson, "A digital communications network for computers giving rapid response at remote terminals," ACM Symp. Operating Systems
Problems, Oct. 1967.

[6]. R. A. Scantlebury, P. T. Wilkinson, and K. A. Bartlett, "The design of a message switching Centre for
a digital communication network," in Proc. IFIP Congress 1968, vol. 2-Hardware Applications," pp. 723-733.

[7]. R. E. Kahn and W. R. Crowther, "Flow control in a resource-sharing computer network," in Proc.

Second ACM/IEEE Symp. Problems, Palo Alto, CA, pp. 108-116, Oct. 1971.

[8]. S. M. Ornstein, F. E. Heart, W. R. Crowther, S. B. Russell, H. K. Rising, and A. Michel, "The terminal

IMP for the ARPA computer network," In AFIPS Conf. Proc. 40, pp. 243-254, June 1972.

[9]. H. Frank. R. E. Kahn, and L. Kleinrock, "Computer communications network design-Experience with theory and practice," in AFIPS Conf. Proc., vol. 40, pp. 255-270, June 1972.

[10]. L. Kleinrock, "Performance models and measurement of the ARPA computer networks," In Proc. Int. Symp. Design and Application of Interactive Computer Systems, Brunel University. Uxbridge,

England, May 1972.

[11] S. Tandel, C. de Launois, C-BGP Home Page, http://cbgp.info.ucl.ac.be/.

[12] F. Hao, P. Koppol, An Internet scale simulation setup for BGP, Computer Communication Review 33 (3) (2003) 43.57.

[13]http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

[14]http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/index.htm

[15] Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall, Fourth Edition, 2002.

[16] William Stallings, *Data and Computer Communications*, Prentice Hall, Eight editions, 2006.

**Mohammad Zunnun Khan** having more then 3 years of experience as a teacher in Integral University, Lucknow, teaching Under Graduate and Post Graduate courses of Engineering and Computer Applications. Presently employed as an **Assistant Professor** in **Computer Science and** Engineering Department of **INTEGRAL UNIVERSITY**, LUCKNOW

**Prof.(Dr.) Mohd Rizwan Beg having** More then 12 years of experience as a teacher, research work, presently **Professor** and Head in **Computer Science and** Engineering Department of **INTEGRAL UNIVERSITY**, LUCKNOW

**Mohd. Shahid Husain having** More then 5 years of experience as a teacher, research work, presently employed as an **Assistant Professor** in **Computer Science and** Engineering Department of **INTEGRAL UNIVERSITY**, LUCKNOW