East West University

Department of Electronics & Communications

Engineering

TE- 598

Title

Comparative Performance Analysis of Static and BGP

Route in a Network using Network Simulator (NS2)

Submitted By

Afroza Shultana Tonny

ID: 2013-3-98-007

APPROVAL

This is to certify that the MS thesis report on "Comparative Performance Analysis of Static and BGP Route in a Network using Network Simulator (NS2) " submitted for the partial fulfillment of the MS degree in Telecommunication Engineering, Electronics and Communication Engineering from the East West University, has been carried out by Afroza Shultana Tonny, bearing ID: 2013-3-98-007, under my supervision. To the best of my knowledge and as per his declaration, the whole work and the complete thesis report has been prepared by the student and has not been submitted to anywhere else.

The thesis report can be considered for evaluation.

………………………………………….

September 2015

Md. Zahedul Hassan, Ph.D

Bangladesh Atomic Energy Commision

Acceptance

This research report presented to the department of electronics and communication engineering, East West University is submitted in partial fulfillment of the requirement for degree of M.Sc. in Telecommunication Engineering, under complete supervision of the undersigned.

……………………

Dr. Mohamed Ruhul Amin

Professor, Department of ECE

East West University

DECLARATION

I hereby declare that I have completed project on the topic "Comparative Performance Analysis of Static and BGP Route in a Network using Network Simulator (NS2) " as well as prepared as research report to the department of Electronics and Communication Engineering East West university in partial fulfillment of the requirement for the degree of MS in Telecommunication Engineering, Under the course "Research (TE)".

I also declare that no part of this Project and thereof has been or is being submitted elsewhere for the award of any degree.

…………………………

Afroza Shultana Tonny
ID: 2013-3-98-007
Department of ECE
East West University

ABSTRACT

Every small and large organization use computer network to share their resources. The size of network is increasing day by day. They are connecting their network to the public network such as Internet. They are scaling up their network Local Area Network to Metropolitan Area Network even Wide Area Network also. The aim of the proposed thesis is to analysis the network performance for both static and BGP route in a network, compare them finally took the best one and enhance the network performance. For performance analysis I have simulated a network topology for both Static and BGP route using an open source simulator NS2. In this research work two types of routing protocols (Static & BGP) have been analyzed to find their capabilities and deficiencies and suggest the most efficient between them. Analysis reveals that BGP routing protocol is better than Static in terms of throughput and delay.

ACKNOWLEDGEMENT

First and foremost with all my heartiest devotion I am grateful to almighty Allah for blessing me with such opportunity of learning and ability to successfully complete the task.

A special Thanks with honor to my supervisor Md Zahedul Hassan; who was kind enough to allocate his valuable time to provide me with his humble guidance, motivating thought and encouragement.

Table of Contents

List of Table

List of Figure

Chapter-1

Introduction

1. Introduction

One of the many remarkable qualities of the Internet is that it has scaled so well to its current size is very large. The Internet evolved from the inter-connection of independent networks and is still constantly evolving number of networks, relations between them, and their connectivity are changing all the time. With the inter-connection of independent networks (domains), a mechanism is needed to route data between the different domains.

For fixed small size networks, routes can be created statically, but for bigger and constantly changing networks we need a protocol that can create, change, and withdraw routes according to the state of the network at a particular moment. Because of the sheer size of the interconnected networks and the dynamics of changes occurring between them, static routing is not good enough since it cannot adapt itself to these changing conditions.

The Border Gateway Protocol (BGP) is a protocol that allows dynamic route creation and maintenance such that reachability is preserved. In contrast to static routing, BGP can automatically adjust routing configuration based on network path distance information received from other users of the protocol. BGP is a rich protocol that has many ways to sustain nodes or network failures as well as changes in the network topology. The main goal of the protocol is to maintain connectivity between inter-connected networks such that traffic can be routed to its destination.

1.1 BGP Protocol

BGP is a protocol for facilitating communications between routers in different autonomous systems. An autonomous system (AS) is a network or group of networks under a shared technical administration and with common routing policies. Network traffic in an AS is classified as either **local traffic** or **transit traffic**. Local traffic either comes from or terminates in that AS, where either the IP host source address or destination address reside. Any other traffic traversing that AS constitutes transit traffic. A major goal of BGP usage in the Internet is to reduce transit traffic.

BGP should be used under the following circumstances:

• Multiple connections exist to external AS's (such as the Internet) via different providers.

• Multiple connections exist to external AS's through the same provider, but connect via a separate routing policy

1.2 Static Route

Static routing is not really a routing protocol. Static routing is simply the process of manually entering routes into a device's routing table via a configuration file that is loaded when the routing device starts up. As an alternative, these routes can be entered by a network administrator who configures the routes manually. Since these manually configured routes don't change after they are configured (unless a human changes them) they are called 'static' routes. Static routing is the simplest form of routing, but it is a manual process.

Static routing is used when network is very small and the routes will probably never change.

Static routing also does not handle failures in external networks well because any route that is configured manually must be updated or reconfigured manually to fix or repair any lost connectivity.

1.3 Multi-Home Routing for Static vs. BGP Routing

The brief description of multi-homing routing is given below for both static and BGP routing. [1]

1.3.1 Multi-homing with Static Route:

The simplest way to multi-home would be with static routes. This requires that you bring two diverse Internet connections from your ISPs into the same router. There would be a primary static route and a secondary static route. The primary route is used if the main connection is up, and the secondary route would be configured to come up only if the main connection is down.

This option is simple but less scalable than BGP. It works well for organizations that need redundant Internet at a single location.

1.3.2 Multi-homing with BGP

The Border Gateway Protocol (BGP) is the routing protocol used for large networks that are made up of multiple independent routing domains or autonomous systems (AS). The most common network that relies on BGP is the Internet. Each ISP has a unique presence on the Internet identified by an Autonomous System number. In general, BGP determines the best path based on the fewest number of autonomous systems needed to transit before reaching a final destination.

When you require redundancy to the Internet, BGP presents many options that static routing is unable to achieve. These include load-balancing and diversity between hardware, providers, and geographical areas. It also utilizes a TCP/IP connection to communicate with its peers. This allows it to determine the full end-to-end reachability of a peer. Static routing can only monitor an interface locally, and if the connection goes down indirectly upstream, it will not sense the loss of connectivity and deactivate the route.

Benefits of Border Gateway Protocol:

The benefits of BGP are given below

- ✓ **Hardware Redundancy**

  BGP allows you to bring diverse Internet connections into multiple routers. Each router would peer with upstream provider(s) over what is called an E-BGP (external) link. Internally, your routers would peer with each other over an I-BGP (internal) link. This allows them to all be in sync, and to alert each other when a BGP path is down.

- ✓ **Load Balancing**

  If your organization is geographically diverse, BGP will allow you to take in Internet connections to several locations, from several providers all over the world, while maintaining a single "presence" on the internet. It also allows you to load balance between multiple connections and providers. In this scenario you may have certain routes using one connection, while other routes are using an alternative connection. It is common to engineer traffic out a provider that is "closer" to destinations in certain geographical areas, or have less "AS hops" necessary to transit. This allows you to reduce latency and increase application performance.

BGP is much more scalable and flexible for large, multi-campus companies and organizations.

1.4 Motivation

Due to these lacking of static route most of the large organization now shifted from static route to BGP protocol. The main objective of this paper is to comparative analysis and performance measurement between static and BGP protocol in a network. In this paper I have shown the improvement of my company network performance and throughput using BGP protocol instead of static route. For demonstrate this scenario I have compared the Static route results with BGP Protocol which are implied in the same network Topology and found the maximum throughput for BGP protocol. For the simulation I have used Network Simulator 2 (NS2) as simulation software which is the most reliable software for network simulation.

1.5 Organization

The rest of this paper is organized as follows:

Chapter 2: In Chapter 2 discuss about the BGP routing protocol, Basic Operation of BGP, BGP message types, Types of BGP peering, BGP path selection and BGP Database, BGP Route Processing

Chapter 3: In Chapter 3 discuss about topology design, Existing topology, Limitations of Existing Topology, New Topology plan, Resources collections.

Chapter 4: In Chapter 4 shown the simulation for the mentioned topology and analysis the result

Chapter 5: In Chapter 5 concludes the work and a summary result of the work. This chapter also contains some future work

Chapter-2

Overview of Boarder Gateway Protocol (BGP)

2.1 Boarder Gateway Protocol (BGP)

The Border Gateway Protocol is an inter-AS routing protocol (eBGP), additionally it is used for intra-AS routing (iBGP) between BGP speakers within the same AS. The main function of BGP speaking systems is to exchange network reachability information with other BGP speakers. For this BGP uses the reliable transport protocol TCP since this satisfies all of its transport requirements and is available on all hosts and routers today. After a BGP session between two routers has been established using TCP (port 179) they initially exchange their full routing tables. Since BGP is an incremental protocol further messages concerning routing information are only sent on changes. It is part of the class of distance vector protocols; therefore the path selection is based on specific distance metrics for each path advertised. But instead of exchanging cost information as it is usually done by distance vector protocols, BGP exchanges full path information to avoid circles. As BGP is based on policies, which lets each AS determine how to handle messages coming from or going to neighboring ASes, this exchange of full path information is important for autonomous systems to make their policy decisions, which depend on the contractual relationship between corresponding ASes. Policy decisions override BGP's default path selection process, which can have negative effects on BGP convergence but provides a very flexible and adaptable protocol.

2.1.1 AS Number

In order to route a data packet to a particular network, the destination network must be Identified and located. BGP uses Prefix Routing to address networks. Network prefix is a general idea of assigning an identifier to a network in such a manner that for each data packet it is clear whether its destination lies inside a given network. Prefix routing is done between independent domains, also called Autonomous Systems (AS). It is the basic abstraction of independent entities comprising routers, networks, and policies.

BGP can be seen as a protocol that maintains information on how data packets should be routed between different Autonomous Systems. Although an AS may consist of many hundreds of networks and thousands of routers, from an external

point of view its behavior has to be consistent. Every AS has a globally unique number (sometimes referred to as Autonomous System Number, or ASN) associated with it; this number is used in both the exchange of exterior routing information (between neighboring ASes), and as an identifier of the AS itself. ASN is only an identifier.

BGP Autonomous Systems are assigned an Autonomous System Number (ASN), which is a 16-bit number ranging from **1 – 65535**. A specific subset of this range, **64512 – 65535**, has been reserved for private (or internal) use.

BGP's loop prevention mechanism is an autonomous system number. When an update about a network leaves an autonomous system, that autonomous system's number is prepended to the list of autonomous systems that have handled that update. When an autonomous system receives an update, it examines the autonomous system list. If it finds its own system number in that list, the update is discarded.
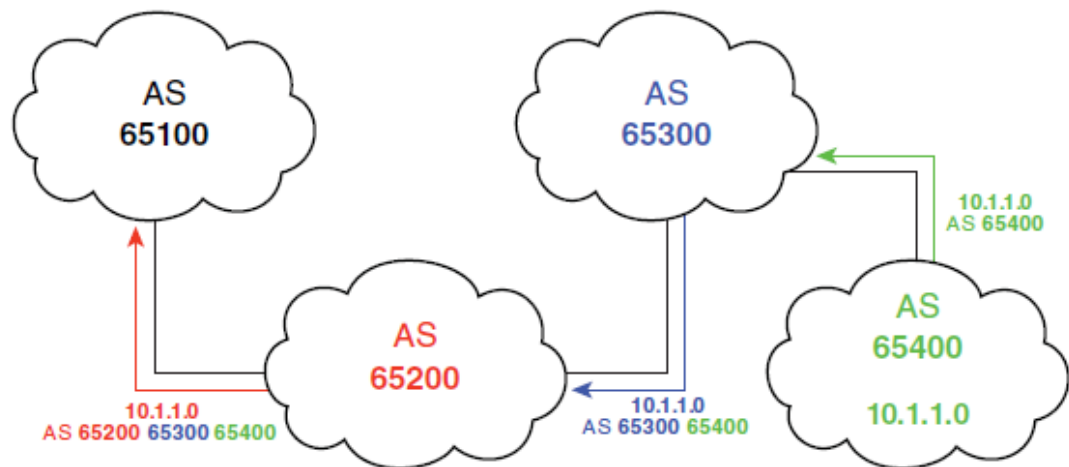
Figure-2.1: BGP AS Path Advertisement

In **Figure-2.1** the BGP routers in AS 65100 see network 10.1.1.0 as having an autonomous system path of 65200 65300 65400.

2.1.2 Types of BGP Peering

For BGP to function, BGP routers (called **speakers)** must form neighbor relationships (called **peers**). [2]

There are two types of BGP neighbor relationships:

- ✓ **iBGP Peers** – BGP neighbors within the same autonomous system.
- ✓ **eBGP Peers** – BGP neighbors connecting separate autonomous systems.

BGP treats updates from internal peers differently than updates from external peers. Before any BGP speaker can peer with a neighbor router, that neighbor must be statically defined.

A TCP session must be established, so the IP address used to peer with must be reachable.

In **Figure-2.2** Routers A and B are EBGP peers. Routers B, C, D are IBGP peers.
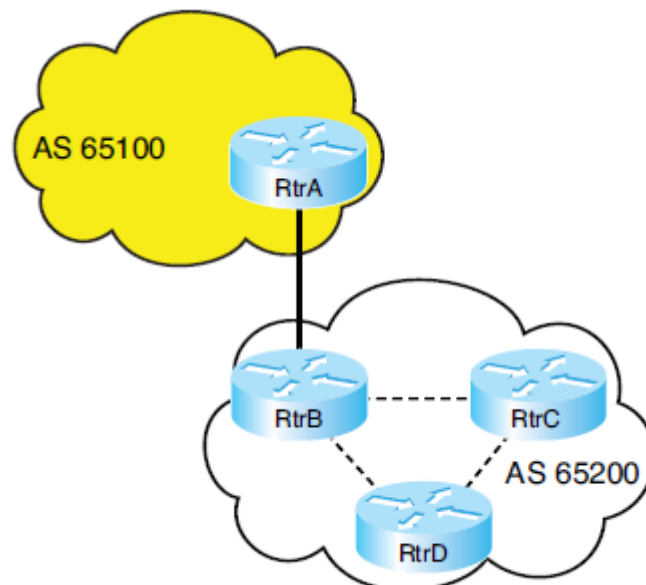
Figure-2.2: Identifying EBGP and IBGP Peers

2.1.3 BGP Message Types

BGP has four types of messages:

- ✓ **Open:** After a neighbor is configured, BGP sends an open message to try to establish peering with that neighbor. Include information such as autonomous system number, router ID, and hold time. [3]
- ✓ **Update:** Message used to transfer routing information between peers. Include new routes, withdrawn routes, and path attributes.
- ✓ **Keep-alive:** BGP peers exchange keep-alive messages every 60 seconds by default. These keep the peering session active.
- ✓ **Notification:** When a problem occurs that causes a router to end the BGP peering session, a notification message is sent to the BGP neighbor and the connection is closed.

2.1.4 BGP Databases

BGP uses three databases. The first two listed are BGP-specific; the third is shared by all routing processes on the router:

Neighbor database: A list of all configured BGP neighbors.

BGP database, or RIB (Routing Information Base): A list of networks known by BGP, along with their paths and attributes.

Routing table: The list of paths to each network used by the router and the next hop for each network.

2.1.5 BGP Finite State Mechanism

As a BGP peer session is forming, it will pass through several **states**. This process is known as the BGP **Finite-State Machine (FSM)**:

Idle – the initial BGP state

Connect - BGP waits for a TCP connection with the remote peer. If successful, an OPEN message is sent. If unsuccessful, the session is placed in an Active state.

Active – BGP attempts to initiate a TCP connection with the remote peer. If successful, an OPEN message is sent. If unsuccessful, BGP will wait for a Connect-Retry timer to expire, and place the session back in a Connect State.

OpenSent – BGP has both established the TCP connection and sent an OPEN Message, and is awaiting a reply OPEN Message. Once it receives a reply OPEN Message, the BGP peer will send a KEEPALIVE message.

OpenConfirm – BGP listens for a reply KEEPALIVE message.

Established – the BGP peer session is fully established. UPDATE messages containing routing information will now be sent.
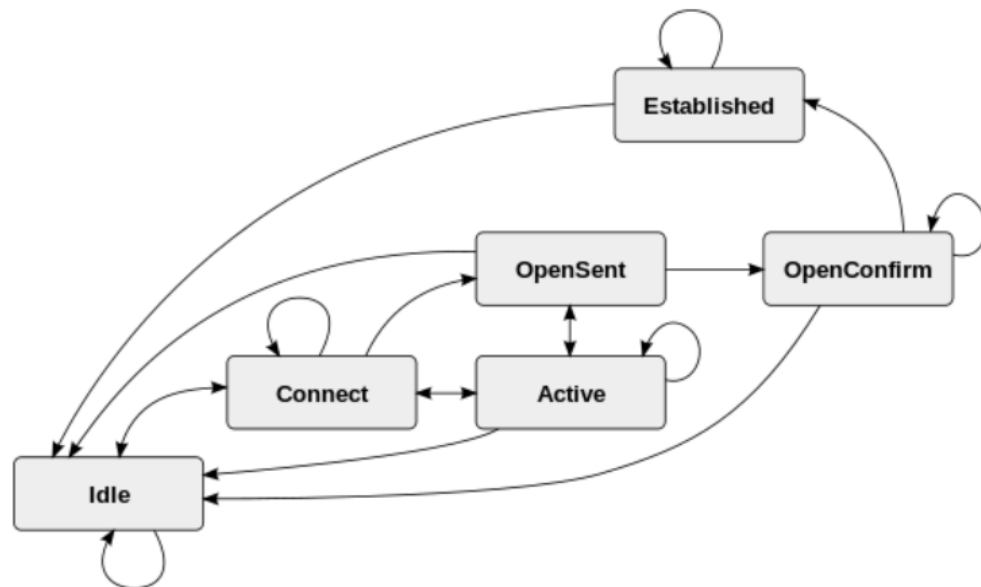
Figure-2.3: BGP Finite State Machine

2.1.6 BGP Next-Hop Selection

The next hop for a route received from an EBGP neighbor is the IP address of the neighbor that sent the update.

When a BGP router receives an update from an EBGP neighbor, it must pass that update to its IBGP neighbors without changing the next-hop attribute.[4] The next-hop IP address is the IP address of an edge router belonging to the next-hop autonomous system. Therefore, IBGP routers must have a route to the network connecting their autonomous system to that edge router. For example, in **Figure-2.4**, RtrA sends an update to RtrB, listing a next hop of 10.2.2.1, its serial interface. When RtrB forwards that update to RtrC, the next-hop IP address will still be 10.2.2.1. RtrC needs to have a route to the 10.2.2.0 network to have a valid next hop. In Figure-4, this configuration goes on RtrB. After you give this command, RtrB advertises its IP address to RtrC as the next hop for networks from AS 65100, rather than the address

of RtrA. Thus, RtrC does not have to know about the external network between RtrA and RtrB (network 10.2.2.0).
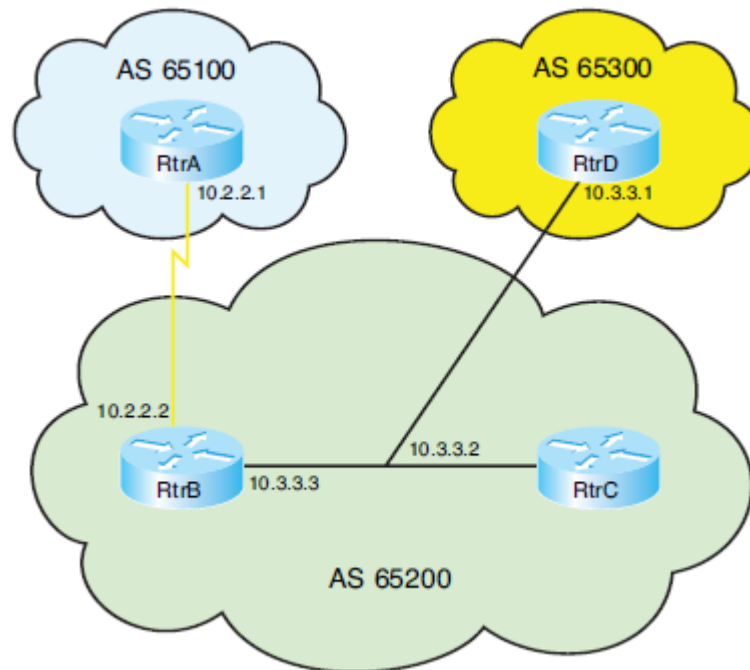
Figure-2.4: BGP Next-Hop Behavior

2.1.7 Basic Operations

BGP is a protocol used for maintaining routing information between ASes. Each AS is connected to a number of other ASes (called neighbors or peers) and exchanges its routes with them according to AS-specific policies. After receiving information an AS may propagate it to its own neighbors.

Most intra-domain routing protocols are based on Dijkstra's algorithm. [5] In contrast, BGP is vector path based, which means that information is not periodically broadcasted and that BGP routers do not have the full topological view of the network. Each router knows only how to reach its direct neighbors and through which neighbor particular Network Prefixes can be reached.

For each Prefix Network, an AS can use only one path as its default path. It can propagate this path to its neighbors, so that they can use the AS as transit for their traffic routing. In addition to the default path, all alternative paths leading to a given Network Prefix received from the other neighbors have to be stored. The reason is to

be able to quickly restore the connectivity when the default path becomes unavailable-an AS may then start to use another path to route data packets and maintain connectivity even when a link has failed or network topology/reachability has changed

2.1.8 BGP Path Selection

BGP, however, has a different way of route selection. It assigns various attributes to each path; these attributes can be administratively manipulated to control the path that is selected. It then examines the value of these attributes in an ordered fashion until it can narrow all the possible routes down to one path.

BGP chooses a route to a network based on the attributes of its path. Four categories of attributes exist as follows:

- ✓ **Well-known mandatory:** Must be recognized by all BGP routers, present in all BGP updates, and passed on to other BGP routers. For example AS path, origin, and next hop.
- ✓ **Well-known discretionary:** Must be recognized by all BGP routers and passed on to other BGP routers but need not be present in an update, for example, local preference.
- ✓ **Optional transitive:** Might or might not be recognized by a BGP router but is passed on to other BGP routers. If not recognized, it is marked as partial, for example, aggregator, community.
- ✓ **Optional non-transitive:** Might or might not be recognized by a BGP router and is not passed on to other routers, for example, Multi-Exit Discriminator (MED), originator ID.

2.1.9 BGP Path Selection Criteria

BGP tries to narrow its path selection down to one best path; it does not load balance by default. To do so, it examines the path attributes of any loop-free, synchronized (if synchronization is enabled) routes with a reachable next-hop in the following order:

- ✓ Choose the route with the highest weight.
- ✓ If weight is not set, choose the route with the highest local preference.
- ✓ Choose routes that this router originated.
- ✓ Choose the path with the shortest Autonomous System path.
- ✓ Choose the path with the lowest origin code (i is lowest, e is next, ? is last).

✓ Choose the route with the lowest MED, if the same Autonomous System advertises the possible routes.

✓ Choose an EBGP route over an IBGP route.

✓ Choose the route through the nearest IGP neighbor as determined by the lowest IGP metric.

✓ Choose the oldest route

✓ Choose a path through the neighbor with the lowest router ID.

✓ Choose a path through the neighbor with the lowest IP address.

2.1.10 BGP Multi-homing

Multi-homing means connecting to more than one ISP at the same time. It is done for redundancy and backup if one ISP fails and for better performance if one ISP provides a better path to frequently used networks. This also gives you an ISP-independent solution. BGP is typically used with multi-homed connections.

Figure-2.5: BGP Multi-homed Network

Configuring a redundant link to the Internet has given my company improved service and has reduced outages and related costs. This strategy also offers network administrators peace of mind as a bonus. Here is how to use Border Gateway Protocol (BGP) to produce similar results for your company.

BGP is one of the key tools for achieving Internet connection redundancy. When you connect your location to two different Internet service providers, it is called multihoming. When you multi-home your network to two different ISPs, BGP runs on

your Internet router(s) and provides redundancy and network optimization by selecting which ISP offers the best path to a resource.

2.1.11 BGP Route Processing

There are two types of BGP peer sessions: external BGP (eBGP) for peers from different ASs and internal BGP (iBGP) for peers from the same AS. A BGP router may receive multiple paths to the same destination prefix from its eBGP and iBGP neighbors. **Figure-2.6** shows the steps of BGP route processing. The router first applies import policies to filter out unwanted routes. For example, a BGP router may only accept advertisements with an AS path containing a set of trusted ASs. The router then invokes a decision process to select exactly one best route for each destination prefix by comparing the new routes to all other known routes to the same destination. The router applies a sequence of steps to narrow the set of candidate routes to a single choice. The best route will be installed in the router's forwarding table, while unselected routes are remembered for backup purposes. Finally, the router applies export policies to manipulate attributes and decide whether to advertise the route to neighboring ASs. If the route is advertised, the router may modify some of the path attributes. It will at least add its own AS number to the AS path.
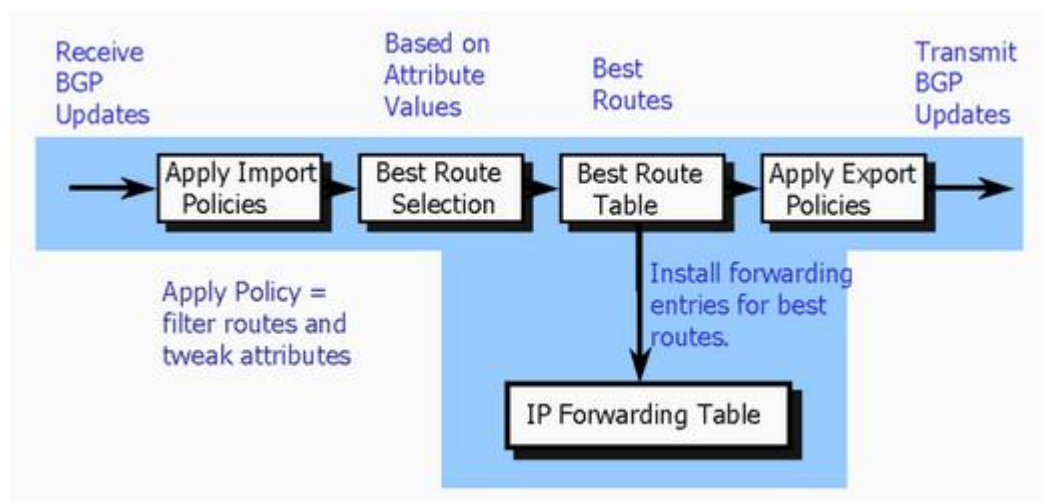

Figure-2.6: BGP route processing

Chapter-3

Design & Implementation

In order to perform simulations using the model designed it has to be implemented as a computer program. There are many ways how the model can be implemented, but in order to achieve the goals-being able to analyze BGP's behavior in large networks-a few that's why I am using Ns-2 to simulate the BGP network.

3.1 Design Objective

I am working corporate office as a network administrator. The size of my corporate network is very large. We have several real-time applications run in my corporate network which has accessed through public IP. Those applications must be available to the user all the time 24X7. Currently my corporate office network uses the traditional static route. The main objective of this design is to replacing the static route with BGP and improves the network performance.

3.2 Existing Design Scenario

The existing network scenario is given below **Figure 3.1**. In the existing topology our **Corporate-Internet-Node-0** is connected to **Internet-Service-Provider-1** and **Corporate-Internet-Node-2** connected to **Internet-Service-Provider-3** and the Branches are connected through the Internet**. Corporate-Internet-Node-0** is also connected service provider node 3 and **Corporate-Internet-Node-2** connected with **Internet-Service-Provider-1 as well** This is a partial sample of our existing network diagram. I have availed same amount of bandwidth from the different ISP. For Internet redundancy and better performance my company has took internet connection from different ISP. Static route is used for reachability.
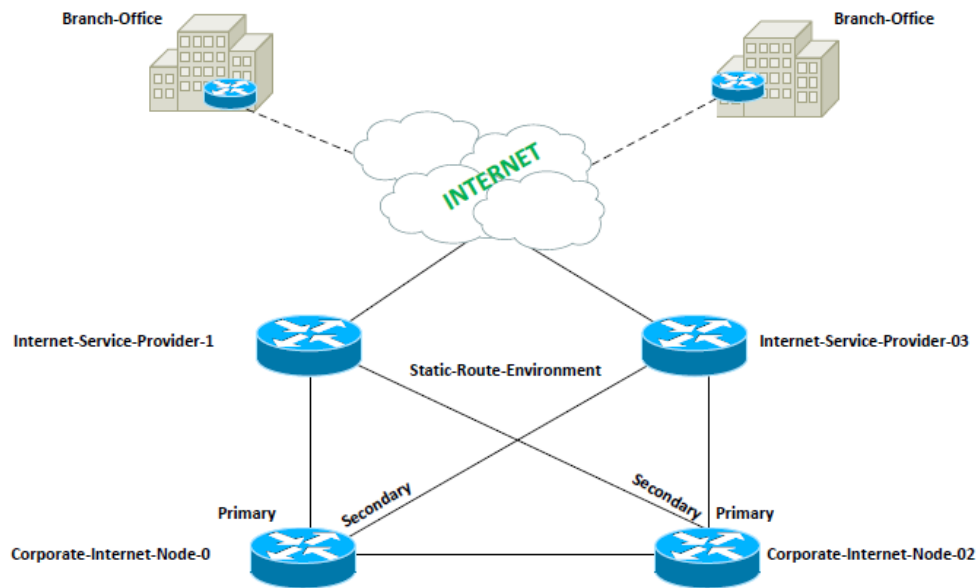
Figure-3.1: Existing Network Diagram

3.2.1 Limitations of Existing Network

✓ In this existing network we have avail same amount of bandwidth from different Internet-Service-Provider use only one service provider bandwidth at a time.

✓ Due to use of static route one router is active at a time.

✓ Waste 50% of total Bandwidth

✓ There is no active-active redundancy. The secondary connection only works when the primary connection is down because Using static route it's not possible to do active-active link redundancy.

✓ User can't utilize maximum throughput against bandwidth.

✓ No route policy can be impose

✓ It's not a scalable solution

3.3 Proposed Network Design Using BGP

The proposed diagram is shown in **Figure-3.2**.
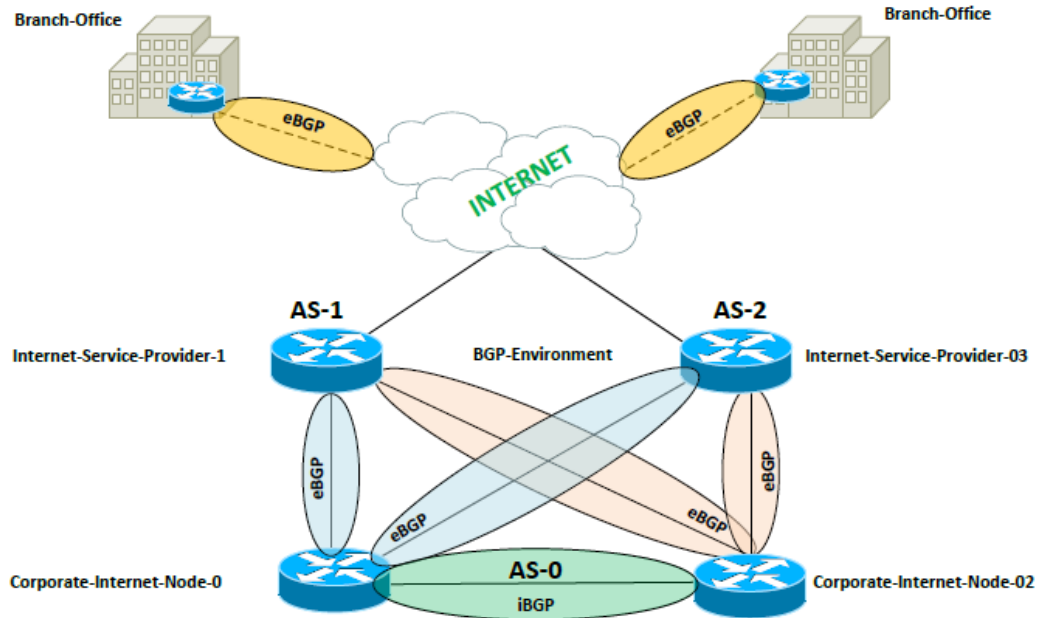
Figure-3.2: Proposed Network Diagram

In the proposed network the topology is remaining same only I have replaced routing protocol. Instead of Static Route I have implemented BGP in the network and improve network performance.

In this topology our **Corporate-Internet-Node-0** is connected to **Internet-Service-Provider-1** and **Corporate-Internet-Node-2** connected to **Internet-Service-Provider-3** and the Branches are connected through the Internet. Connection Types are given below:

- ✓ Corporate-Internet-Node-0-To-Internet-Service-Provider-1-----eBGP Peering
- ✓ Corporate-Internet-Node-2-To-Internet-Service-Provider-3----- eBGP Peering
- ✓ Corporate-Internet-Node-0-To- Corporate-Internet-Node-0------iBGP Peering
- ✓ Branch-Office-To-Corporate-Internet-Node-Connection-Via------eBGP Peering

3.3.1 Advantages of Proposed Network over Existing Network

✔ In this existing network we have avail same amount of bandwidth from different Internet-Service-Provider both service provider are active and utilize bandwidth of both service provider.

✔ Provide Hardware Redundancy BGP allows bringing diverse Internet connections into multiple routers. Each router would peer with upstream provider(s) over what is called an E-BGP (external) link. Internally, routers would peer with each other over an I-BGP (internal) link. This allows them to all be in sync, and to alert each other when a BGP path is down.

✔ It allows load balancing

✔ Use 100% bandwidth. No ISP connection is remaining IDLE.

✔ User can utilize maximum throughput against bandwidth.

✔ Also impose the route policy and improve the network performance.

✔ There is active-active link redundancy is possible.

Chapter-4

Simulation & Results

To begin with at first I have simulated my corporate network topology using Static Route. I have measured the throughput against bandwidth from each node to node. Then I have simulated BGP for the same parameters where topology is remaining same and then I compared the results between them to get a decision.

4.1 Ns-2 Network Simulator

I have implemented ns-BGP as an extension to the latest version of ns-2 network simulator (ns-2.35) ns-2 being an open source simulator has the advantage over other simulators like Graphical Network Simulator (GNS) that its files are easy to modify and source files are freely available which was developed at the ISI (University of Southern California). It was originally developed as an extension to the REAL network simulator. As one of the most popular discrete event network simulators, ns-2 supports simulation of TCP, routing, and multicast protocols over wired and wireless networks. ns-2 is written in both C++ and OTcl and employs an object-oriented paradigm. C++ is used for the low level implementation of packet oriented processing, where performance is important. OTcl is a scripting language used for higher level implementation, where flexibility is more important. A graphical animator nam is used to visualize simulation results. We can implement new protocol in NS2 easily. GNS require extra files like .iso files for specific router. We cannot modify files in GNS like we can in NS2. For network researchers and students NS2 is the best available simulation tool. So I used NS2 for my simulation.

4.2 Design Consideration

In my paper I have consider two routing protocol implement in a same network and calculate the throughput and compare them. First of all I have simulated the Static Route in my company network then simulated the BGP for the same. At the end I have briefly analyses the result for the both option. For testing the maximum throughput against I have consider the different level of Bandwidth and delay for throughput testing.

4.3 Topology for Static Route

At first for comparison purpose I have shown the existing topology and simulation. In my topology (as shown in Figure-4.1) for static route **node 0** and **node 2** is considered as my office part node. **Node 1** and **node 3** considered as service provider end. **Node 1 and Node 3** considered as my destination. For better understanding I have used node color Blue for my corporate office node My have several branches all over the world here I have shown only the Internet service provider portion for the clear concept.
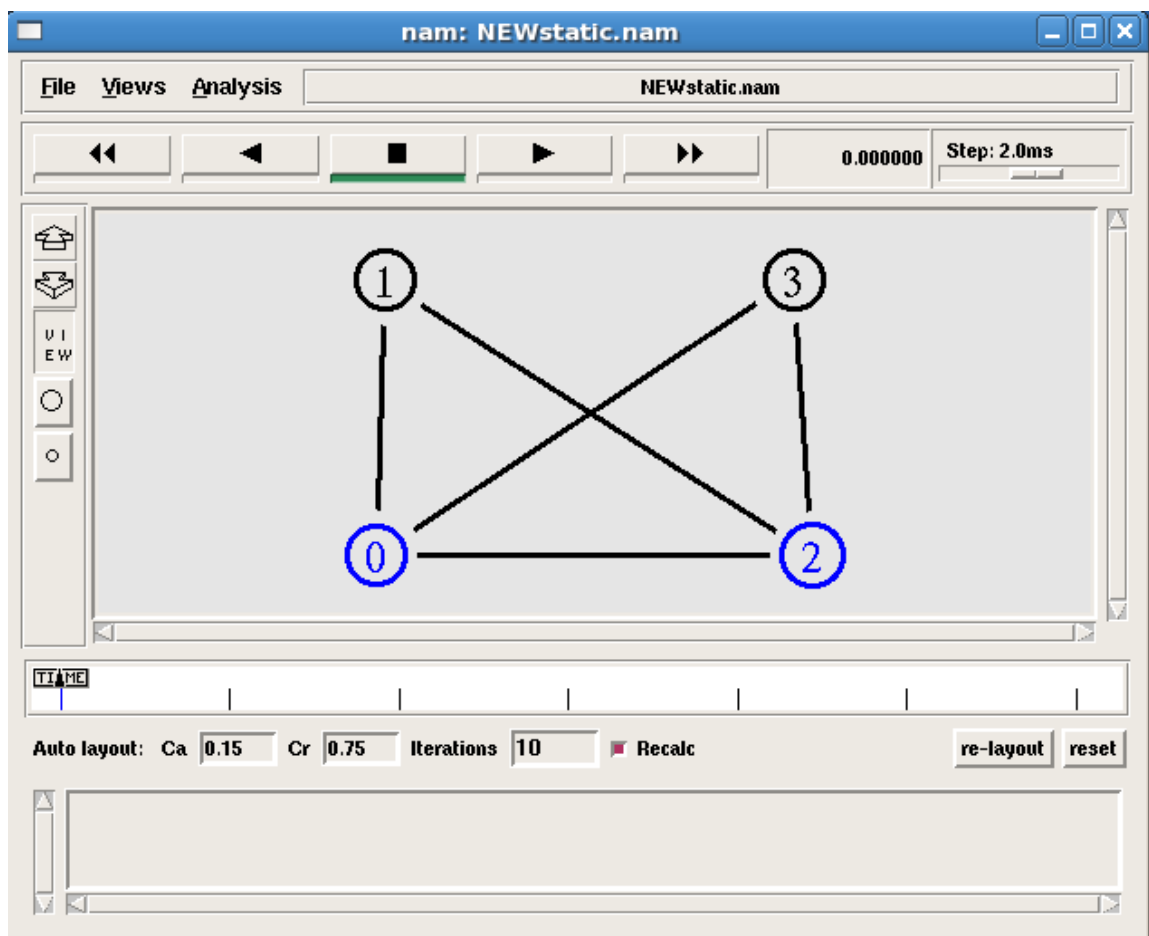
Figure-4.1: Existing Topology for Static Route-1

4.3.1Throughput Calculation for Static Route

In the following figure there 3 parallel path from my corporate office to outside world. One is 0-1-another is 0-3 and 0-2-1 or 0-2-3 One is primary uplink and one is backup uplink and rest of the one is work only when both primary and secondary uplink is down. For better understanding of the network I have taken equal distance between all adjacent nodes the bandwidth of all links are also similar. **Figure-4.2** shows the communication between node 0 and node 1. We can see that the primary path is node 0-1.

Figure-4.2: Traffic originating path from node 0 to node 1

Table-4.1: Throughput calculation from node 0 to node 1

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-1	1.5Mbps	10ms	64.02Mb
Node 0 –To-Node-1	1.0Mbps	10ms	49.80Mb
Node 0 –To-Node-1	0.5Mbps	10ms	32.54Mb

Figure-4.3 shows the communication between node 0 and node 3. We can see that secondary path is node 0-3.
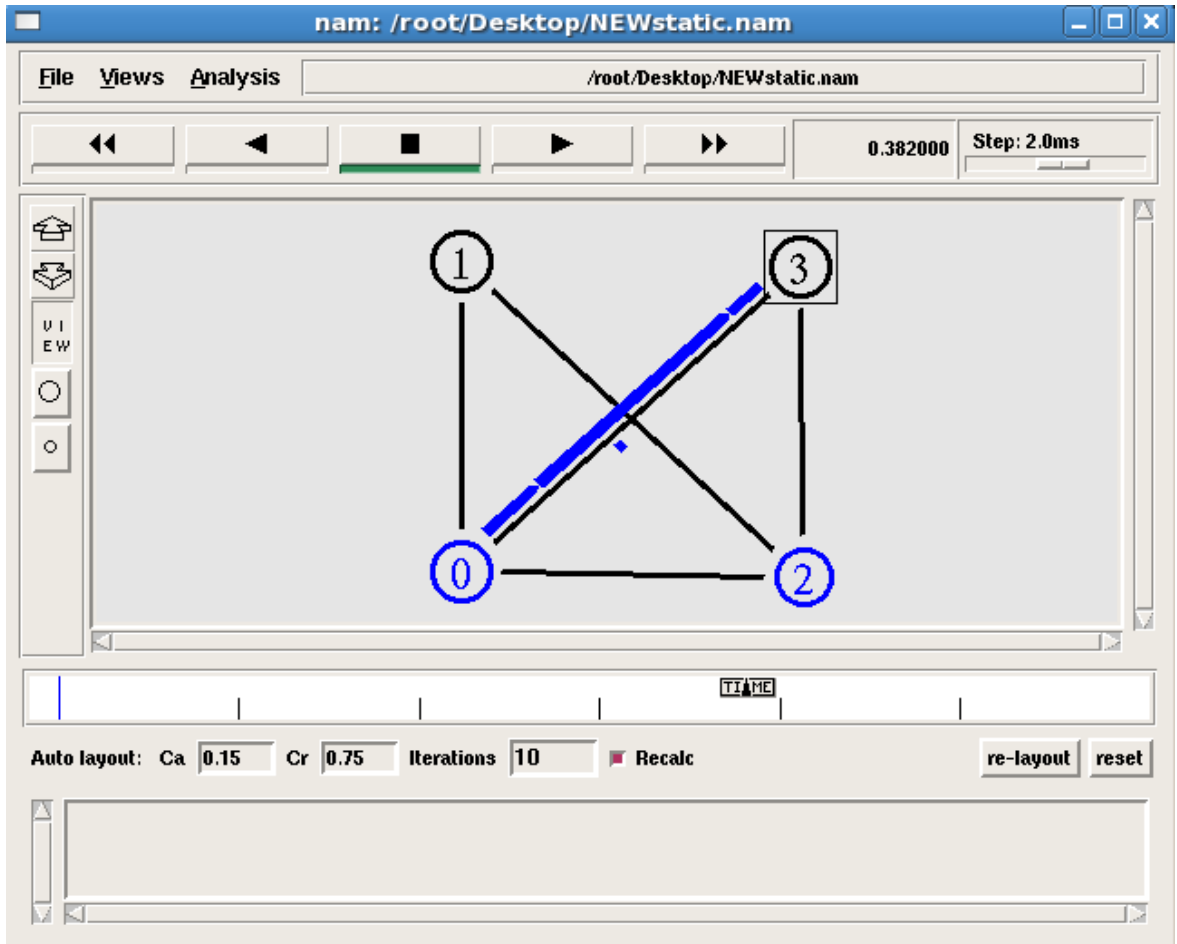
Figure-4.3: Traffic originating path from node 0 to node 3

Table-4.2: Throughput calculation from node 0 to node 3

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-3	1.5Mbps	10ms	64.02Mb
Node 0 –To-Node-3	1.0Mbps	10ms	49.80Mb
Node 0 –To-Node-3	0.5Mbps	10ms	32.54Mb

Figure-4.4 shows the communication between node 2 and node 1. We can see that secondary node path is 2-1.
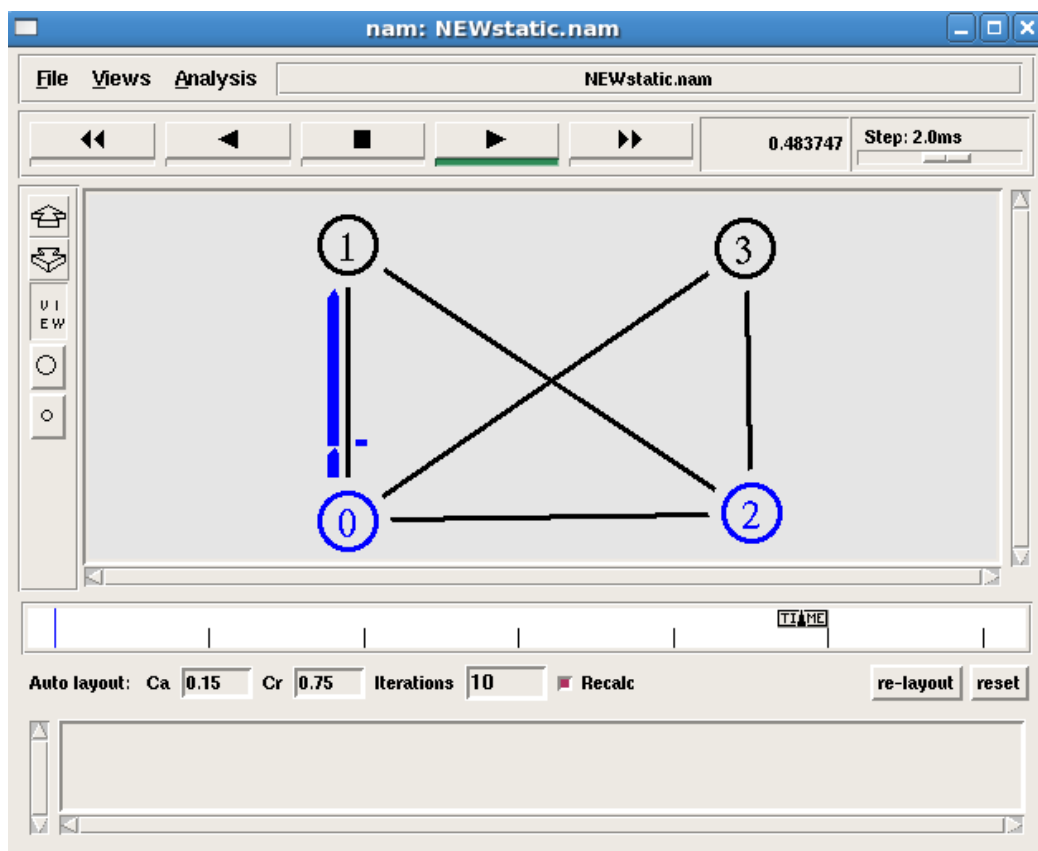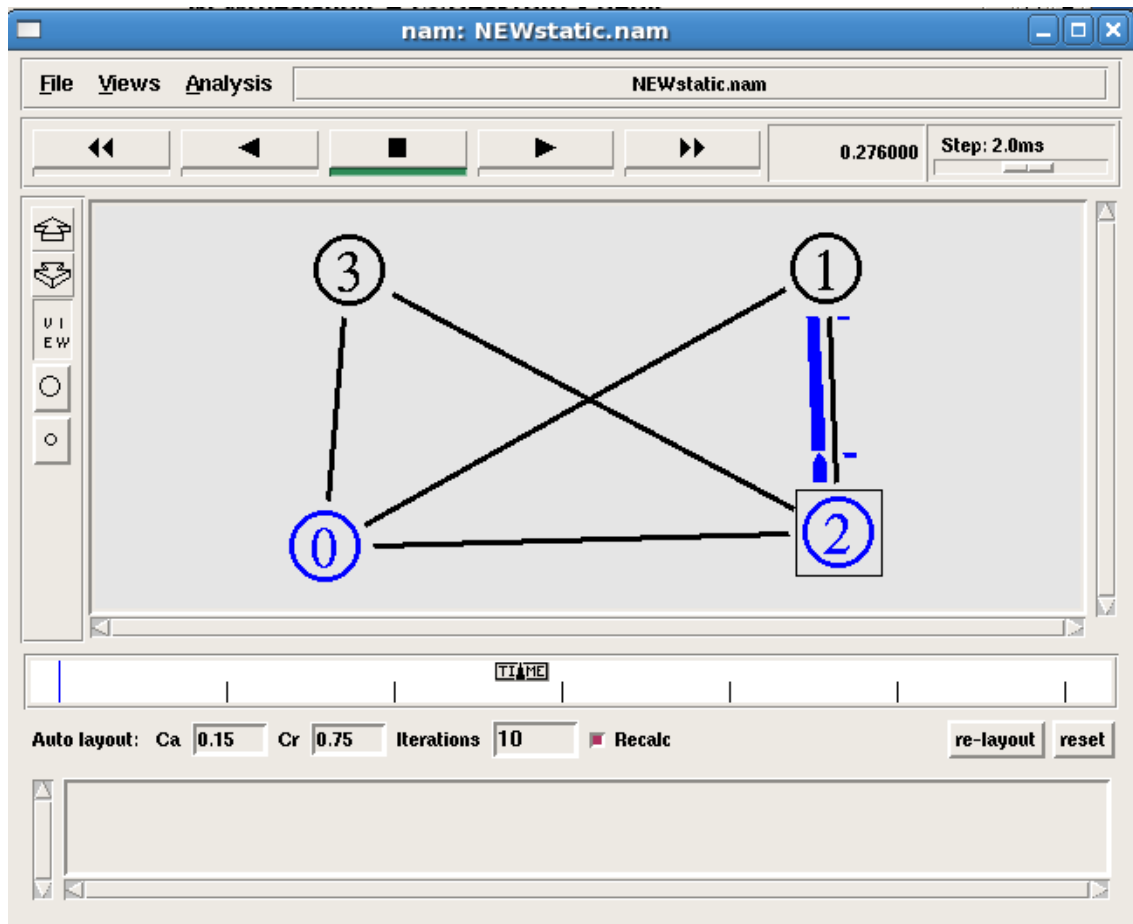

Figure-4.4: Traffic originating path from node 2 to node 1

Table-4.3: Throughput calculation from node 2 to node 1

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 2 –To-Node-1	1.5Mbps	10ms	64.02Mb
Node 2 –To-Node-1	1.0Mbps	10ms	49.80Mb
Node 2 –To-Node-1	0.5Mbps	10ms	32.54Mb

For the above scenarios I have got the same throughput because the bandwidth and delay is same.

4.3.2 Throughput for different delay Condition in Static Route

Now in below I have shown the different types of delay condition for the same bandwidth from node 0-To-node-1. In both situation I have changed the delay value the bandwidth are same for the both scenario. These below table show the different throughput value for different delay condition.

Table-4.4: Throughput calculation from node 0 to node 1 using different delay and bandwidth

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-1	1.5Mbps	100ms	2.07 Mb
Node 0 –To-Node-1	1.0Mbps	50ms	6.13 Mb
Node 0 –To-Node-1	0.5Mbps	10ms	32.53Mb

Table-4.5: Throughput calculation from node 0 to node 1 using different delay

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-1	0.01Mbps	100ms	3.08Mb
Node 0 –To-Node-1	0.01Mbps	50ms	3.08Mb
Node 0 –To-Node-1	0.01Mbps	10ms	4.10Mb

4.3.3 Static Route Path Selection

Figure-4.5 shows the path from node0 to node1 which is the default or primary path for existing topology.
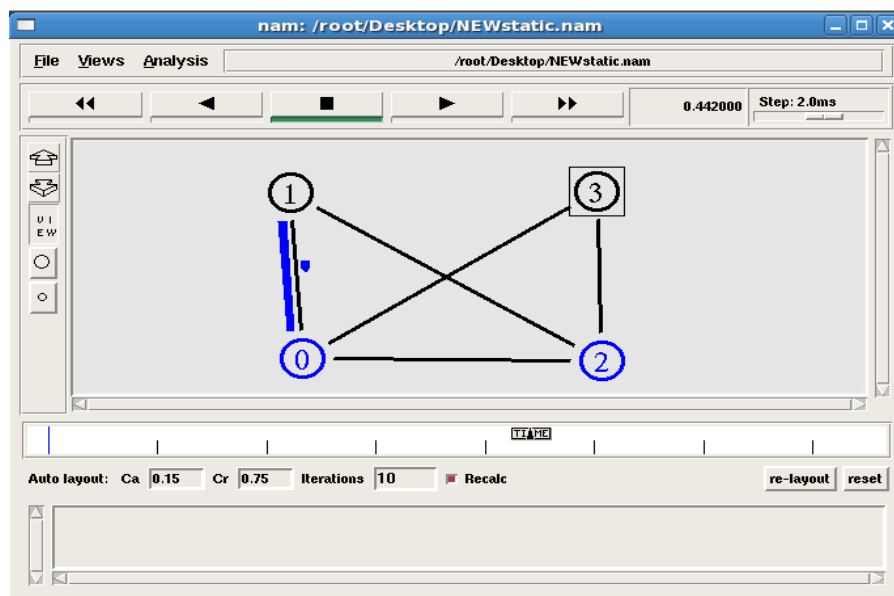
Figure-4.5: Default path from node 0 to node 1

The above path is primary path by default all the route goes through that path. In this case node0 to node 3 bandwidth is not used it's remain IDLE. I can't utilize maximum bandwidth.

Figure-4.6 shows the path from node0 to node3 which is the secondary path for existing topology. This secondary path is work only when
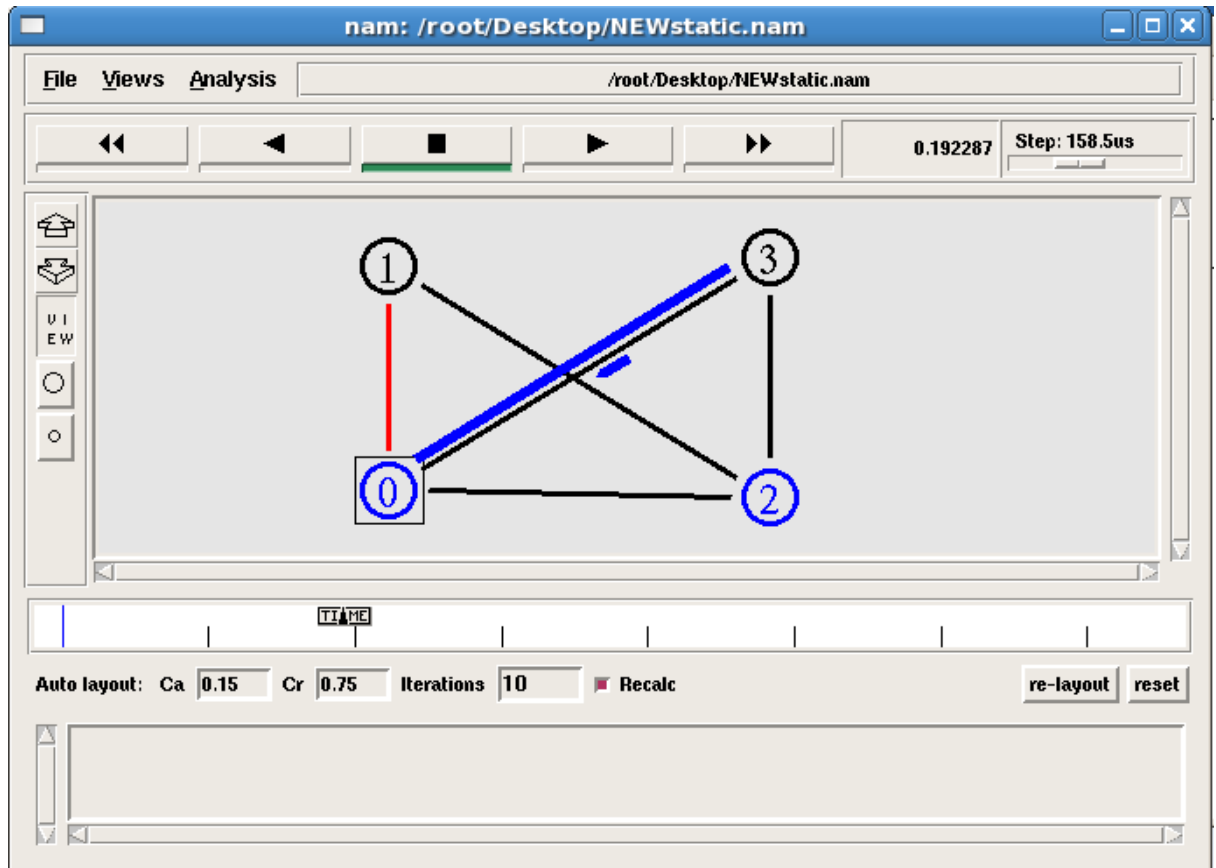
Figure-4.6: Secondary path from node 0 to node 3

This link 0-3 is a backup connection. But this backup connection process traffic only when the link between node 0 and node 1 is down. For this reason only one ISP is used.

Figure-4.7 shows the path from node0 to node3 connection via node 2. In this scenario traffic take the path 0-2-3. This will happen only when both link between node 0-node 1 and node 0-node 3 down.
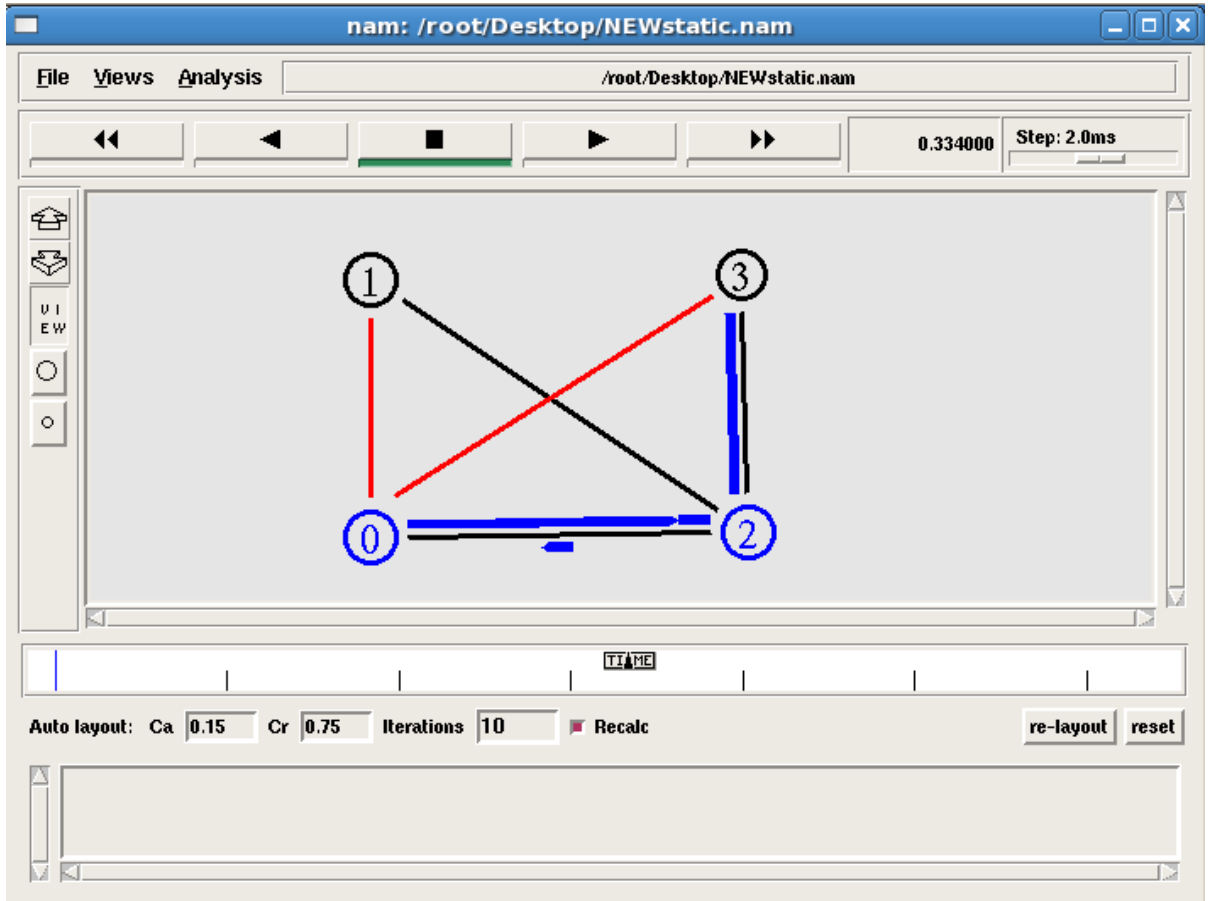
Figure-4.7: Traffic path from node 0 to node 3 via node 2

Table-4.6: Throughput calculation from node 0 to node 3 during link down condition

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-3	0.3Mbps	10ms	20.35Mb
Node 0 –To-Node-3	0.3Mbps	40ms	8.16Mb

Figure-4.8 shows the path from node0 to node3 connection via node 2. In this scenario traffic take the path 0-2-3. This will happen only when both link between node 0-node 1 and node 0-node 3 down.
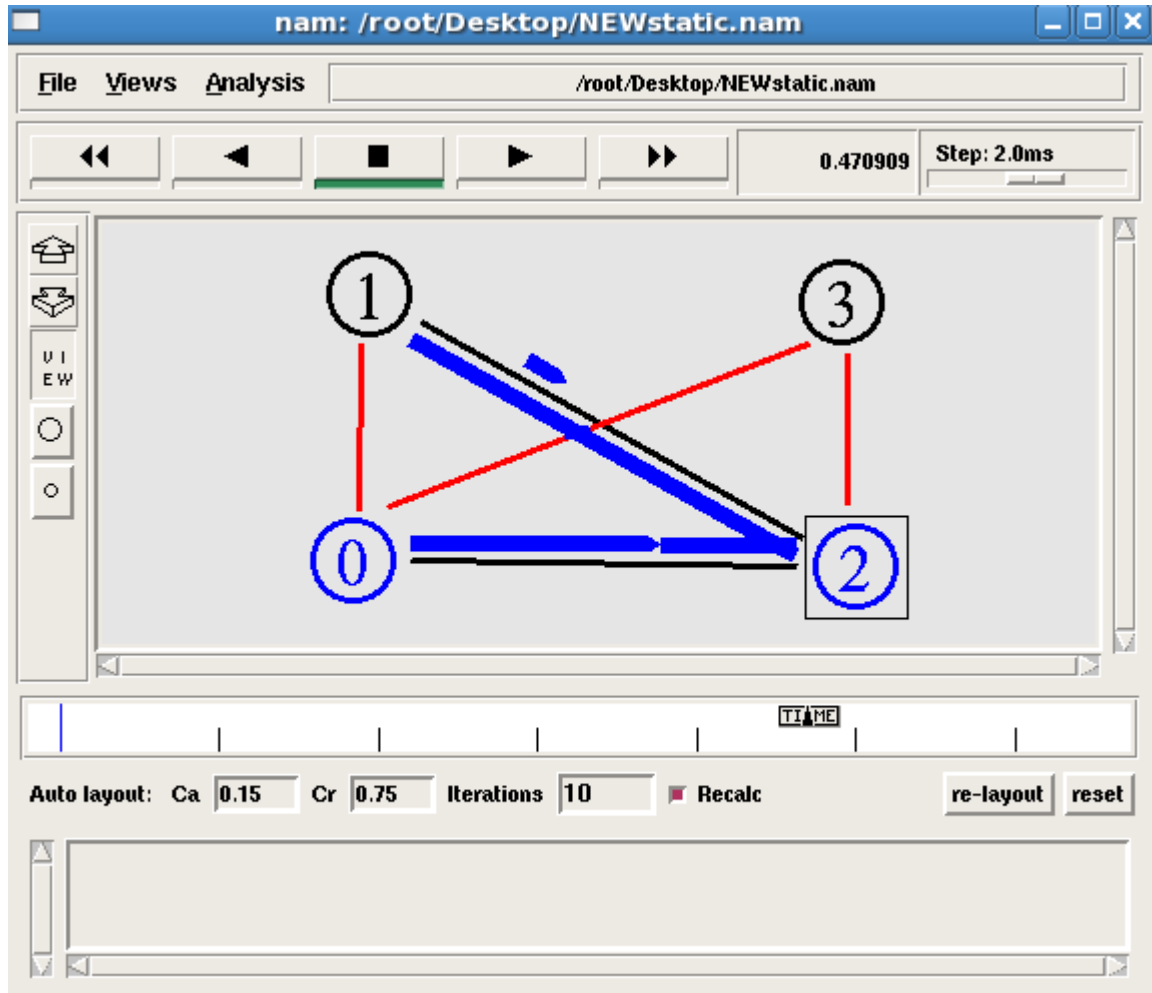
Figure-4.8: Traffic path from node 0 to node 1 via node 2

Table-4.6: Throughput calculation from node 0 to node 1 during link down condition

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-1	0.3Mbps	10ms	20.35Mb
Node 0 –To-Node-1	0.3Mbps	40ms	8.16Mb

Each time of link failure the static route take manual intervention. During link failure situation rote is not shifted to secondary dynamically its must be changed manually.

I have considered the same network topology for BGP. Now at first simulate the BGP and then calculate the throughput for the same parameter as I have mentioned above. Let's simulate and validate test for the same corporate network.

4.4 Route selection validation test

This test checks whether a BGP speaker chooses routes properly when there is more than one path to a particular destination. BGP bases its decision on the values of path attributes. Following is an ordered list of rules used to determine the best path (also shown in Figure 2.2):

- ✓ prefer the path with the largest Local Preference
- ✓ prefer the path with the shortest AS path
- ✓ prefer the path with the lowest multiple exit discriminator (MED)
- ✓ prefer external (eBGP) over internal (iBGP) paths
- ✓ prefer the path with the lowest IGP metric to the BGP next hop.

Since the Local Preference path attribute is not considered in this validation test, the best route will be the route with the shortest AS path.

4.4.1 Network topology

Figure 4.9 shows the network topology used for the simulation of route selection. The network consists of three ASs. Each AS contains one node: AS 0 contain node 0 and node 2, AS 1 and AS2 contain node 1 and node 3 respectively. The IP address of each node is shown in Table-4.7.

Table-4.7: IP addresses used in the route selection validation test.

Node	AS-Number	IP-Address
Node 0	AS 0	10.0.0.1
Node 1	AS 1	10.0.1.1
Node 2	AS 0	10.0.2.1
Node 3	AS 2	10.0.3.1
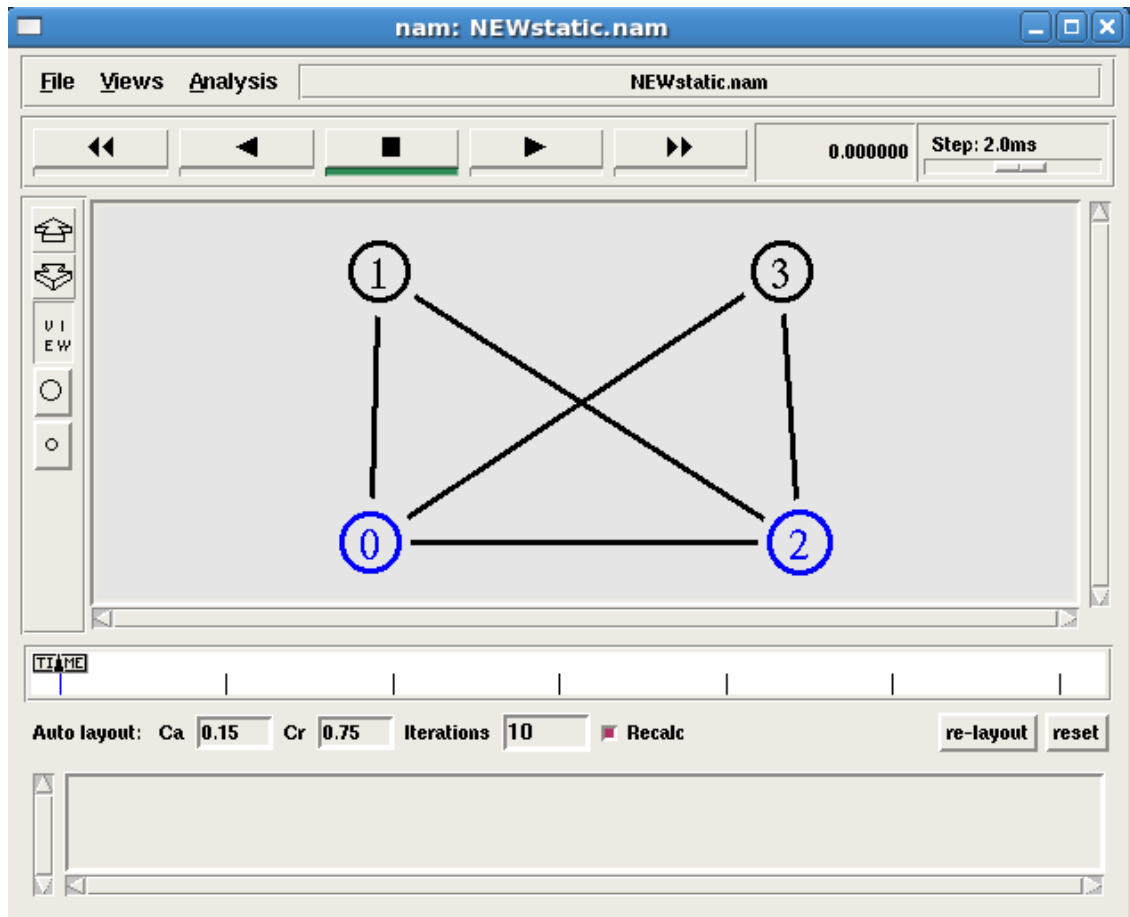
Figure 4.9: Network topology used in the BGP route selection validation test.

4.4.2 BGP configuration and event scheduling

BGP agents are configured for each of the three nodes (0, 1, 2 and 3). External BGP (eBGP) connections exist between nodes 0 and 1, 0 and 3, 2 and 1, as well as 2 and 3. Internal BGP (iBGP) connection exist between nodes 0 and 2. At 0.15 s, the BGP agent in node 0 advertises a new route for IP address 10.0.0.0/24. At 0.16 s, the BGP agent in node 1 advertises a new route for IP address 10.0.1.0/24. At 0.20 s, the BGP agent in node 2 advertises a route for IP address 10.0.2.0/24. At 0.30s the BGP agent in node 3 advertises a route for IP address 10.0.3.0/24. 55.0 s, ns-2 displays all routing tables from BGP agents. The simulation terminates at 58.0 s.

4.4.3 Simulation results

The simulation sequence of events is shown below. Simulation results displayed by nam are Figure-4.10.

time: 0.15

n0 (ip_addr 10.0.0.1) defines a network 10.0.0.0/24

time: 0.25

n1 (ip_addr 10.0.1.1) defines a network 10.0.1.0/24

time: 0.35

n2 (ip_addr 10.0.2.1) defines a network 10.0.2.0/24

time: 0.45

n3 (ip_addr 10.0.3.1) defines a network 10.0.3.0/24

Figure 4.10: Snapshots of nam simulation results of reconnection test.

time: 50
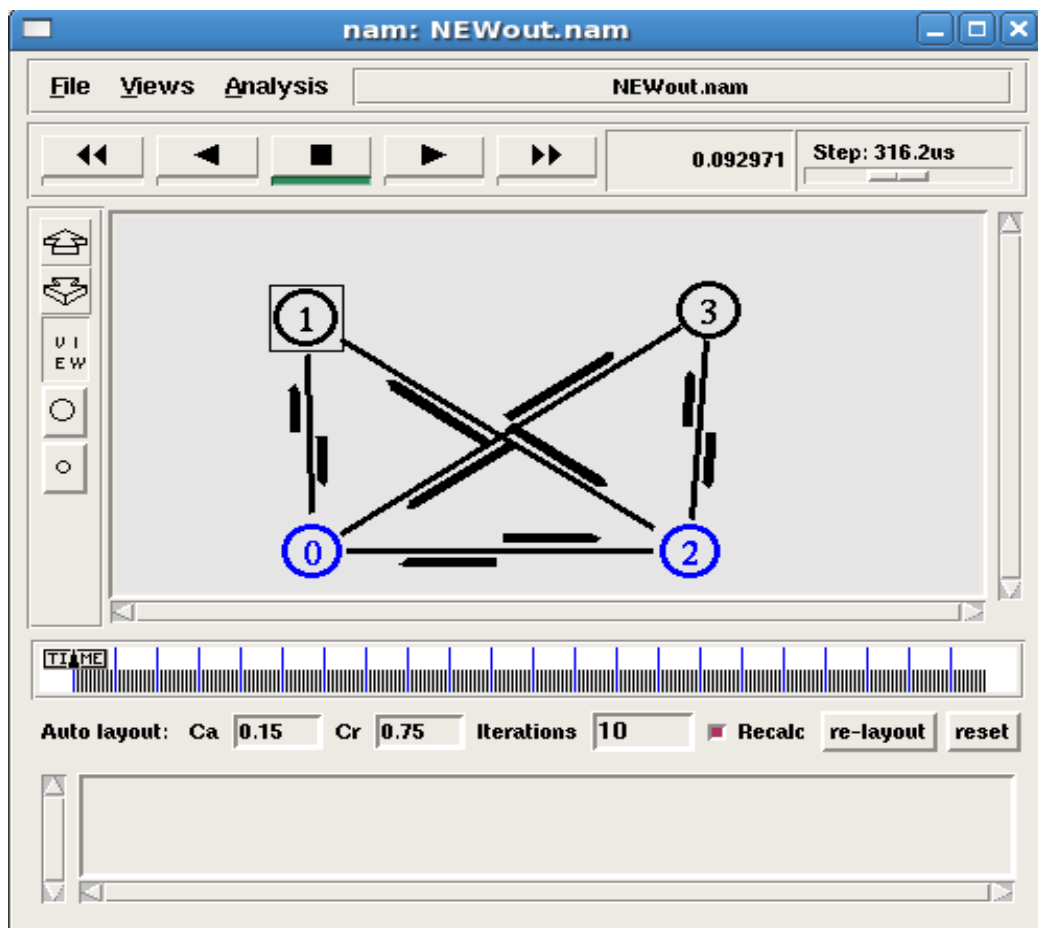
 dump routing tables in all BGP agents:

BGP routing table of n0

BGP table version is 6, local router ID is 10.0.0.1

Status codes: * valid, > best, i - internal.

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.0.0/24	self	-	-	-	
*> 10.0.1.0/24	10.0.1.1/32	-	-	-	1
*> 10.0.3.0/24	10.0.3.1/32	-	-	-	2

BGP routing table of n1

BGP table version is 7, local router ID is 10.0.1.1

Status codes: * valid, > best, i - internal.

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.0.0/24	10.0.0.1/32	-	-	-	0
*> 10.0.1.0/24	self	-	-	-	
*> 10.0.2.0/24	10.0.2.1/32	-	-	-	0
*> 10.0.3.0/24	10.0.0.1/32	-	-	-	0 2

BGP routing table of n2

BGP table version is 4, local router ID is 10.0.2.1

Status codes: * valid, > best, i - internal.

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.1.0/24	10.0.1.1/32	-	-	-	1
*> 10.0.2.0/24	self	-	-	-	
*> 10.0.3.0/24	10.0.3.1/32	-	-	-	2

BGP routing table of n3

BGP table version is 5, local router ID is 10.0.3.1

Status codes: * valid, > best, i - internal.

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.0.0/24	10.0.0.1/32	-	-	-	0
*> 10.0.1.0/24	10.0.0.1/32	-	-	-	0 1
*> 10.0.2.0/24	10.0.2.1/32	-	-	-	0
*> 10.0.3.0/24	self	-	-	-	

4.4.4 Throughput Calculation for BGP

For throughput calculation I have used the same parameter as the Static Route. Generate the traffic from source node 0 and node 2 to the destination node 1 and node 3 as well.
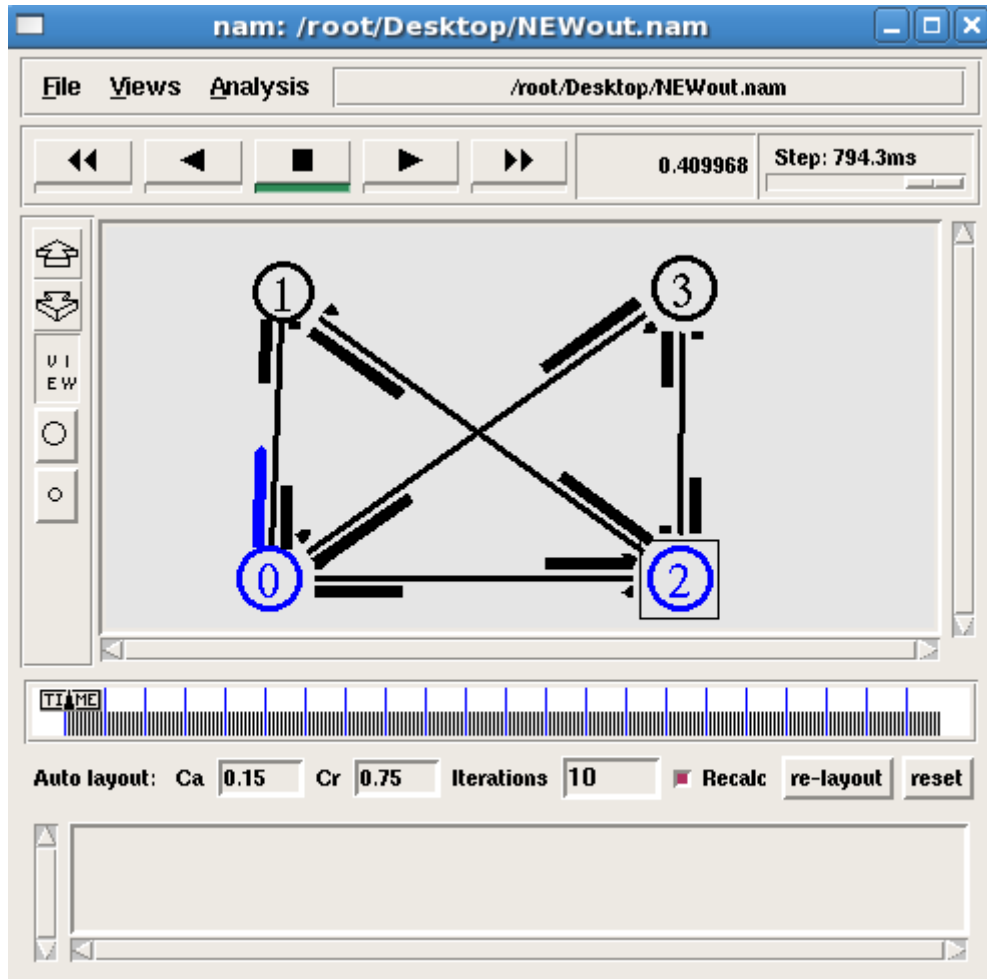
Figure 4.11: Traffic originating path from node 0 to node 1

Here both the ISP is active and exchanges their routing with the neighbor according to table shown above. So we can utilize the bandwidth of both ISP. No ISP is remaining in IDLE state. By using BGP we can utilize the maximum number of bandwidth. We get the same throughput when we consider the traffic path from node 0-3, 2-1, 2-3. I have shown only for node 0 to node1 throughput result.

Table-4.8: Through calculation from node 0 to node1 in BGP route

Node to Node Communication	Bandwidth	Delay	Throughput(Maximum Data Transfer in 55s)
Node 0 –To-Node-1	1.5Mbps	10ms	64.73Mb
Node 0 –To-Node-1	1.0Mbps	10ms	50.52Mb
Node 0 –To-Node-1	0.5Mbps	10ms	33.32Mb

By comparing the value to throughput from Table-4.1 and Table 4.8 we can get the maximum throughput.

4.4.5 Throughput for different delay Condition in BGP Route

Now in below I have shown the different types of delay condition for the same bandwidth from node 0-To-node-1. In both situation I have took delay and the bandwidth are same according to Static Route. These below table show the different throughput value for different delay condition.

Table-4.9: Throughput calculation from node 0 to node 1 using different delay and bandwidth

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	1.5Mbps	100ms	2.853Mb
Node 0 –To-Node-1	1.0Mbps	50ms	7.013Mb
Node 0 –To-Node-1	0.5Mbps	10ms	34.12Mb

Table-4.10: Throughput calculation from node 0 to node 1 using different delay

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	0.01Mbps	100ms	4.10Mb
Node 0 –To-Node-1	0.01Mbps	50ms	4.26Mb
Node 0 –To-Node-1	0.01Mbps	10ms	4.47Mb

4.5 Result Analysis

The result analysis is given below. After result comparison and analysis I have took the decision

4.5.1 Throughput Comparison for different Bandwidth

Now I want to compare my finding together to get a complete picture. For this purpose at first I compared the throughput of the traffic path node0-node1 where I have considered different bandwidth but delay is same for all. I will calculate the throughput for both Static and BGP. I have calculated the throughput for the Figure-4.1 (Static Route) and Figure-4.11(BGP Route). And comparison of throughput chart is shown in Figure-4.12.

Static Route Throughput for different Bandwidth:

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	1.5Mbps	10ms	64.02Mb
Node 0 –To-Node-1	1.0Mbps	10ms	49.80Mb
Node 0 –To-Node-1	0.5Mbps	10ms	32.54Mb

BGP Throughput for different Bandwidth:

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	1.5Mbps	10ms	64.73Mb
Node 0 –To-Node-1	1.0Mbps	10ms	50.52Mb
Node 0 –To-Node-1	0.5Mbps	10ms	33.32Mb

For testing I have consider the delay 10ms only changes the bandwidth for both BGP and Static Route.
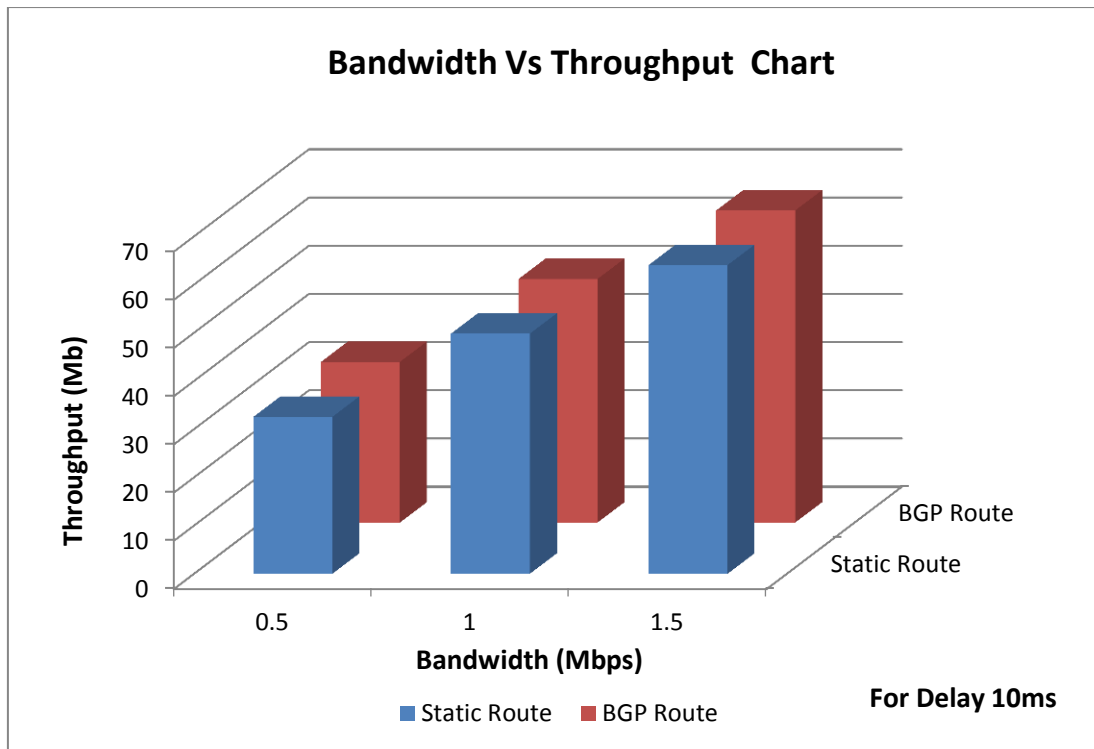
Figure 4.12: Bandwidth Vs Throughput chart for Static and BGP Route

From the Figure-4.12 it is clear that I have got better throughput for BGP route than Static Route. The testing parameter is same for both Static and BGP Route.

4.5.2 Throughput Comparison for different Delay

Another important parameter for real time communication is delay time. Figure-4.13 shows the throughput calculation in delay condition. Here I have considered different delay time but Bandwidth is same for all.

Static Route Throughput for different delay condition:

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	0.01Mbps	100ms	3.08Mb
Node 0 –To-Node-1	0.01Mbps	50ms	3.08Mb
Node 0 –To-Node-1	0.01Mbps	10ms	4.10Mb

BGP Route Throughput for different delay condition:

Node to Node Communication	Bandwidth	Delay	Throughput
Node 0 –To-Node-1	0.01Mbps	100ms	4.10Mb
Node 0 –To-Node-1	0.01Mbps	50ms	4.26Mb
Node 0 –To-Node-1	0.01Mbps	10ms	4.47Mb

For testing I have consider the bandwidth 0.01M only changes the delay for both BGP and Static Route
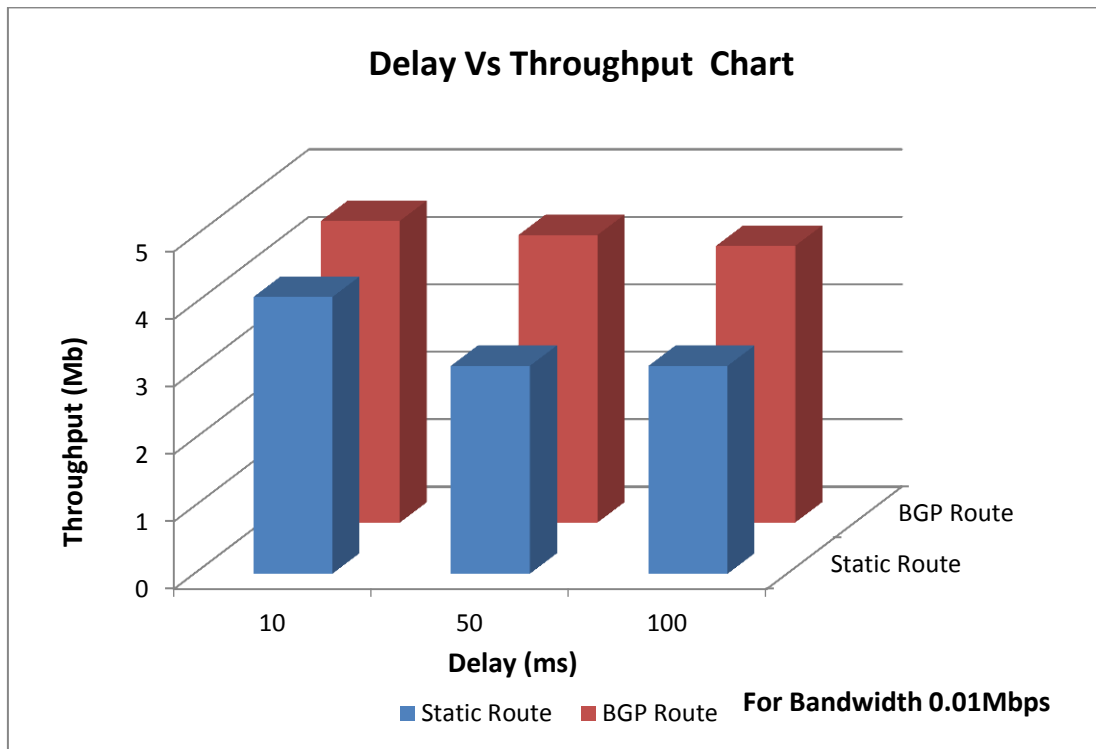
Figure 4.13: Delay Vs Throughput chart for Static and BGP Route

From the Figure-4.13 it is also clear that BGP has work better and give better throughput than static when delay occur in my network.

Chapter-5

Conclusion

In this paper I tried to find a suitable routing protocol for my office network topology which is useful for real time communication. In real time communication there are few very important parameters that make it hard for normal packet based network to give as acceptable QOS. These parameters are End to End delay, link failure condition and throughput.

1st I have simulated the static route calculate the throughput. For maximum throughput calculate I have considered the different bandwidth and delay. Then simulated the BGP route for the same topology and calculate the throughput for the same parameter. I have found that BGP protocol provides the maximum throughput for any circumstances than static route as I have discussed in the previous chapter. By using the BGP protocol I can increase my network performance 38.29% in delay condition. I have found that for 0.5Mbps, 1Mbps and 1.5 Mbps BGP can increase the throughput 2.4%, 1.57% and 1.22% respectively. In delay condition for 10ms, 50ms and 100ms BGP can increase the throughput 9.05%, 38.29% and 33.16%. And for link failure condition where static route require manual intervention for link restoration BGP can automatically shift the traffic from the failure link to available link. So I have got a better performance in every aspect by using BGP in my office network topology. By using BGP I can also utilize the both ISP bandwidth. For using BGP both ISP is active traffic can be pass any of the path. BGP also give me active-active redundancy for ISP.

As for feature work, more realistic network topologies and routing polices can be employed to simulate genuine behavior of the Internet. Additional features, such as route flap damping, policy routing, and multiprotocol extension, may be added to the existing ns-BGP model. These features will help compare the performance of various algorithms for route flap damping, study the detailed behavior of BGP policy routing, and evaluate new technologies that are based on the multiprotocol extension, such as BGP/MPLS (Multiprotocol Label Switching) VPN (virtual private network).

Reference

[1]http://www.syringanetworks.net/resources/industry_library/internet_redundancy__

multi-homing_with_bgp_or_static_routing/

[2] Aaron Balchunas BGP v2.012007

[3] Aaron Balchunas BGP v2.012007

[4] Cisco CCNP Route 642-902 Quick Reference

[5] Maciej Wojciechowski, thesis_bgpsim

Appendix

<u>TCL code for Static Route in Ns2</u>

```
#Create a Simulator Object
set ns [new Simulator]


#Define  Different Color For the Data Flow
$ns color 1 Blue


#Protocol Static
$ns rtproto Static


#Create Four Nodes
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]


#Define the NAM Node Color For My Corporate office Node Color is Blue
$n0 color blue
$n2 color blue


#Open the Name Trace File
set f [open NEWstaticout.tr w]
$ns trace-all $f
set nf [open NEWstatic.nam w]
$ns namtrace-all $nf


#Create links between the nodes
$ns duplex-link $n0 $n1 1Mb 10ms DropTail
$ns duplex-link $n0 $n2 1Mb 10ms DropTail
$ns duplex-link $n0 $n3 1Mb 10ms DropTail
$ns duplex-link $n2 $n1 1Mb 10ms DropTail
$ns duplex-link $n2 $n3 1Mb 10ms DropTail
```

#Give node position (for NAM)

$ns duplex-link-op $n0 $n2 orient right

$ns duplex-link-op $n0 $n1 orient up

$ns duplex-link-op $n2 $n3 orient up

#Color

$ns duplex-link-op $n0 $n1 color "red"

$ns duplex-link-op $n0 $n3 color "red"

Create a TCP agent and connect it to an application like FTP or Telnet, which

generates the data

##setup a TCP Connection

set tcp [new Agent/TCP]

$ns attach-agent $n0 $tcp

set sink [new Agent/TCPSink]

$ns attach-agent $n1 $sink

$ns connect $tcp $sink

$tcp set fid_ 1

##setup a FTP over TCP connection

set ftp [new Application/FTP]

$ftp attach-agent $tcp

$ftp set type_ FTP

##Schedule events for the FTP agents

$ns at 0.10 "$ftp start"

$ns at 0.40 "$ftp stop"

#Call the Finish Procedure after 60 Sec of the Simulation Time

$ns at 60.0 "finish"

#Define a Finish Procedure

```
proc finish {} {
    global ns f nf
    $ns flush-trace
    close $f
 close $nf

    puts "running nam..."
    exec nam NEWstatic.nam &
    exit 0
}

$ns run
```

TCL code for BGP Route in Ns2

```
#Create a Simulator Object
set ns [new Simulator]


#Define  Different Color For the Data Flow
$ns color 1 Blue
$ns color 2 Red


#Protocol BGP
$ns node-config -BGP ON
set n0 [$ns node 0:10.0.0.1]
set n1 [$ns node 1:10.0.1.1]
set n2 [$ns node 0:10.0.2.1]
set n3 [$ns node 2:10.0.3.1]
$ns node-config -BGP OFF


#Define the NAM Node Color For My Corporate office Node Color is Blue
$n0 color blue
$n2 color blue


#Open the Name Trace File
set f [open NEWout.tr w]
$ns trace-all $f
set nf [open NEWout.nam w]
$ns namtrace-all $nf


#Create links between the nodes
$ns duplex-link $n0 $n1 1Mb 10ms DropTail
$ns duplex-link $n0 $n2 1Mb 10ms DropTail
$ns duplex-link $n0 $n3 1Mb 10ms DropTail
$ns duplex-link $n2 $n3 1Mb 10ms DropTail
```

$ns duplex-link $n2 $n1 1Mb 10ms DropTail

#Give node position (for NAM)

$ns duplex-link-op $n0 $n2 orient right

$ns duplex-link-op $n0 $n1 orient up

$ns duplex-link-op $n2 $n3 orient up

#Define BGP Agent

set bgp_agent0 [$n0 get-bgp-agent]

$bgp_agent0 bgp-id 10.0.0.1

$bgp_agent0 neighbor 10.0.1.1 remote-as 1

$bgp_agent0 neighbor 10.0.2.1 remote-as 0

$bgp_agent0 neighbor 10.0.3.1 remote-as 2

set bgp_agent1 [$n1 get-bgp-agent]

$bgp_agent1 bgp-id 10.0.1.1

$bgp_agent1 neighbor 10.0.0.1 remote-as 0

$bgp_agent1 neighbor 10.0.2.1 remote-as 0

set bgp_agent2 [$n2 get-bgp-agent]

$bgp_agent2 bgp-id 10.0.2.1

$bgp_agent2 neighbor 10.0.0.1 remote-as 0

$bgp_agent2 neighbor 10.0.3.1 remote-as 2

$bgp_agent2 neighbor 10.0.1.1 remote-as 1

set bgp_agent3 [$n3 get-bgp-agent]

$bgp_agent3 bgp-id 10.0.3.1

$bgp_agent3 neighbor 10.0.0.1 remote-as 0

$bgp_agent3 neighbor 10.0.2.1 remote-as 0

Create a TCP agent and connect it to an application like FTP or Telnet, which

generates the data

```
#setup a TCP Connection
set tcp [new Agent/TCP]
$ns attach-agent $n0 $tcp
set sink [new Agent/TCPSink]
$ns attach-agent $n1 $sink
$ns connect $tcp $sink
$tcp set fid_ 1


##setup a FTP over TCP connection
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ftp set type_ FTP


##Schedule events for the FTP agents
$ns at 0.10 "$ftp start"
$ns at 0.40 "$ftp stop"


# Define Shcedule for BGP
$ns at 0.15 "puts \"\n time: 0.15 \n n0 (ip_addr 10.0.0.1) \ defines a network
10.0.0.0/24 \""
$ns at 0.15 "$bgp_agent0 network 10.0.0.0/24"


$ns at 0.25 "puts \"\n time: 0.25 \n n1 (ip_addr 10.0.1.1) \ defines a network
10.0.1.0/24 \""
$ns at 0.25 "$bgp_agent1 network 10.0.1.0/24"


$ns at 0.35 "puts \"\n time: 0.35 \n n2 (ip_addr 10.0.2.1) \ defines a network
10.0.2.0/24 \""
$ns at 0.35 "$bgp_agent2 network 10.0.2.0/24"


$ns at 0.45 "puts \"\n time: 0.45 \n n3 (ip_addr 10.0.3.1) \ defines a network
10.0.3.0/24 \""
$ns at 0.45 "$bgp_agent3 network 10.0.3.0/24"
```

```
$ns at 55.0 "puts \"\n time: 50 \
\n dump routing tables in all BGP agents: \n\""
$ns at 55.0 "$bgp_agent0 show-routes"
$ns at 55.0 "$bgp_agent1 show-routes"
$ns at 55.0 "$bgp_agent2 show-routes"
$ns at 55.0 "$bgp_agent3 show-routes"


#Call the Finish Procedure after 60 Sec of the Simulation Time
$ns at 60.0 "finish"
proc finish {} {
    global ns f nf
    $ns flush-trace
    close $f
    close $nf

    puts "running nam..."
    exec nam NEWout.nam &
    exit 0
}
$ns run
```

<u>AWK code to analyse trace file</u>

```awk
BEGIN

    { th=0; th1=0; th2=0;

     dr=0 }

#packet delivery ratio

{
    if($1=="+" && $3=="0" && $4=="1" ) {th=th+$6;}

    if($1=="-" && $3=="0" && $4=="1" ) {th1=th1+$6;}

    if($1=="r" && $3=="0" && $4=="1" ) {th2=th2+$6;}

    if($1=="d" && $3=="0" && $4=="1" ) {dr=dr+$6;}
}


END

    {

            printf("Total enque:=%d\n",th); printf("Total deque:=%d\n",th1);

            printf("Total receive:=%d\n",th2); printf("Total drop:=%d\n",dr);


        }
```