GEO BASED ROUTING FOR BORDER GATEWAY PROTOCOL IN ISP MULTI-HOMING ENVIRONMENT

Duleep Thilakarathne
(118473A)

Degree of Master of Science

Department of Electronic and Telecommunication Engineering

University of Moratuwa
Sri Lanka

November 2015

GEO BASED ROUTING FOR
BORDER GATEWAY PROTOCOL
IN ISP MULTI-HOMING ENVIRONMENT

Duleep Thilakarathne

(118473A)

Thesis Submitted in Partial Fulfillment of the Requirements for the Degree Master of Science in Telecommunication

Department of Electronic and Telecommunication Engineering

University of Moratuwa
Sri Lanka

November 2015

Declaration

I declare that this is my own work and this thesis/dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: Date:

The above candidate has carried out research for the Masters Dissertation under my supervision.

Signature of the supervisor: Date

Abstract

GEO BASED ROUTING FOR BORDER GATEWAY PROTOCOL IN ISP MULTI-HOMING ENVIRONMENT

Key words: BGP, SDN, AS-PATH, optimum route selection, Internet Architecture, Internet routing, Latency

BGP is the one and only protocol used by ISPs to exchange routing information between Autonomous Systems. An Autonomous System is an IP network or group of IP networks under a common administration with common routing policies. Internet Service Providers (ISP) connects to each other to facilitate reachability among Autonomous Systems using BGP protocol.

Many ISPs setup multiple upstream connections to achieve global connectivity, redundancy, and a better quality of service. Multiple upstream connectivity results multiple paths to destinations. ISPs need to apply complex route policies to select the best outgoing interface to destination among multiple paths since BGP protocol does not consider link congestion, and distance to destination during the route selection process. Incorrect path selection leads to unnecessary traffic route between autonomous systems, high latency and low quality of service. Most prevailing issue for the South Asian internet users is that Internet content is not hosted within the region but in Singapore, Europe, and USA data centers. BGP protocol does not select shortest distance always when multiple upstream connections are available to ISP. This results in high latency to the end users.

We can simulate different ISP path delays by introducing delay element between end server and client terminal. This proposal provides experimental results on how end user experience varies when delay to end server varies. Delay is proportional to distance between user terminal and end server. Therefore, this proposal considers distance to end server when solution is proposed to optimize end user delay. Traditional BGP does not consider geographical distance to end server when selecting outgoing interface. BGP has thirteen criteria to select best outgoing interface but most dominant criteria is the AS-PATH length. This research focuses on equal AS path length occurrences of current full BGP routing table in multi-homing environment. Equal AS-PATH length results BGP protocol to select outgoing interface randomly based on lowest router ID or lowest interface ID. The proposal suggests using geo graphic distance to destination as tiebreak condition for equal AS-PATH. This enables BGP itself to calculate best path without using complex routing policies.

BGP is a heavily adopted protocol in the internet domain. It is hard to change such a stable implementation to achieve proposed geo based routing. SDN based implementation proposes in this proposal since SDN implementation is becoming popular in IP networking domain. New route selection criteria for BGP can easily implement using SDN controller. Simulation results reveal approximately 50 percent of the routing decisions are based on equal AS-PATH length if special routing policies are not applied. Further, simulation result justifies a relationship between latency and web page browsing user experience.

Dedication

This is dedicated to my loving Father and Mother.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Dr. Ajith Pasqual, for the continuous support for my MSC research study, for his patience, motivation, and immense knowledge shared. His guidance helped me at all times of research and writing of this thesis.

Besides my advisor, I would like to thank Dr. Chandika Wavegedara for his insightful comments and encouragement.

My sincere thanks also goes to the senior management of Mobitel (Pvt) limited who provide me access to simulation data. Without ISP environment real-time data, it would not be possible to conduct this research.

I thank my office colleagues who helped and encouraged me during simulations and research case development.

Last but not the least, I would like to thank my family: my wife and daughters for supporting me spiritually throughout writing this thesis.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
AS	Autonomous System
BGP	Border Gateway Protocol
EBGP	Exterior Border Gateway Protocol
IBGP	Interior Border Gateway Protocol
ISP	Internet Service Provider
SDN	Software Define Networking

List of Appendices

Chapter 1

INTRODUCTION

1.1 Internet

Internet is a physical network connecting millions of computers using TCP/IP protocol and packet switching for sharing/transmitting information. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies [1]. Figure 1 illustrates worldwide internet users distribution based on geographic regions.

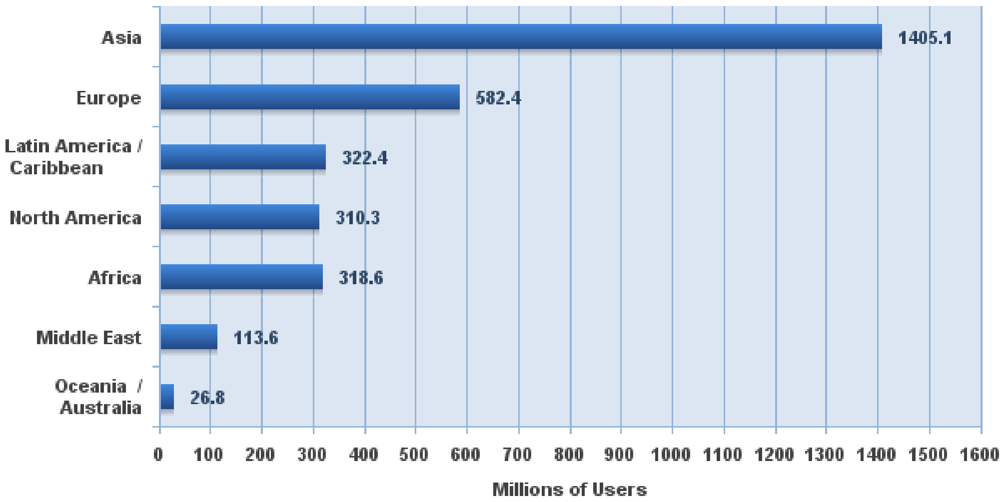

Figure 1: Internet Users in the world by geographic regions

Source: Internet world stats – www.internetworldstats.com/stat.htm

According to Figure 1, highest number of internet users is in Asian region, although most countries in this zone are still developing. This could be due to high population density in the Asian region. However, it is important to note that the highest contribution to growth of internet is from Asian countries. Figure 2 depicts worldwide internet penetration rate based on geographic regions. Accordingly, it is evident that internet user count is high in many regions but user penetration is less than 50 per cent in 5 regions. There could be several reasons for this low penetration. Non-availability of internet connectivity to end user, cost of internet connection, bad end user experience, and insufficient technology awareness are few reasons for low penetration of internet in Asia.

Out of the above reasons, end user experience is an important factor. Several research are conducted on improving internet user experience. End users experience depends on many reasons, and latency is a key factor to Asian countries since most of the content resides in USA and European regions of the world.

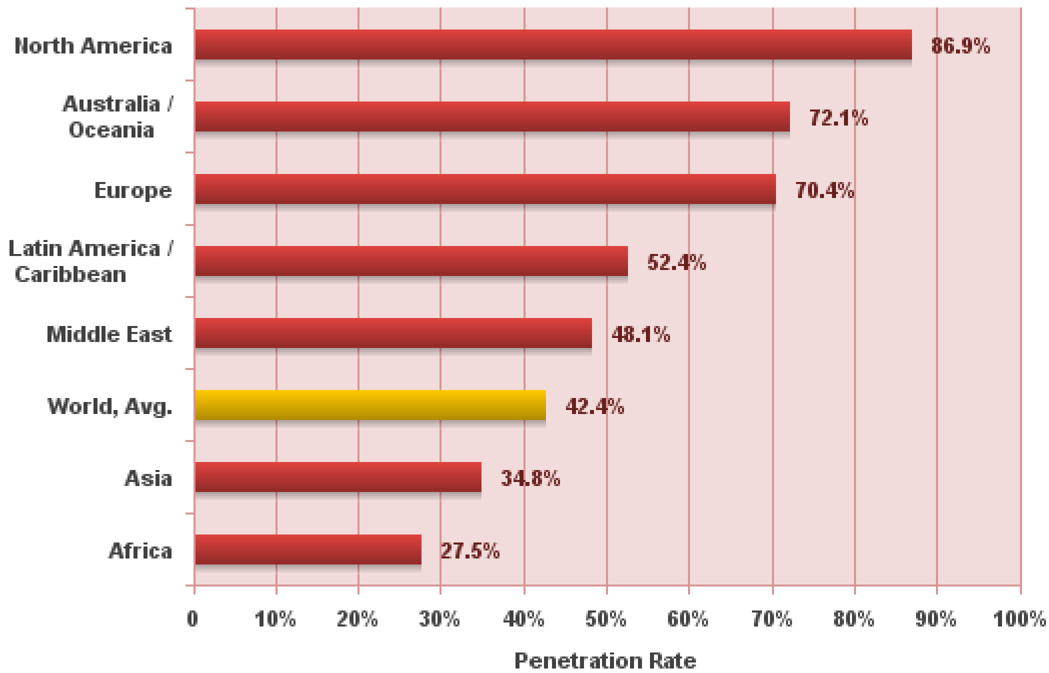

Figure 2: Internet penetration in the world by geographic regions

Source: Internet world stats – www.internetworldstats.com/stat.htm

1.2 Internet Architecture to Reduce Latency

There is a tendency to setup data centers in Singapore region by a majority of content providers to address Asian latency issue. However, latency depends on internet service provider upstream connection topology and how data is transferred from end user to destination. Table 1 presents the time taken to reach web server hosted in three different geographical regions, namely USA, Netherland and Singapore, from Sri Lanka through different upstream internet service providers.

Table 1: Latency to different servers through different ISP

Upstream Provides	Two way delay (ms) to server located at		
	USA	**Europe**	**Asia**
USA	250	250	300
Europe	250	250	300
Asia	300	300	50

Above latency values prove that time taken to reach end server purely depends on upstream internet service provider connectivity and geographic location of the content hosted. Further, latency is proportionate with end user experience. In above scenario, if Sri Lankan ISP connects only to USA region, time taken to reach Asian content is always high compared to USA and Europe region. Most of the giant content providers identify request origination geo region from Domain Name Request (DNS) and reply nearest data center IP address to end user. In such a case, end users receive Asian data center IP for Asian users, European data center IP for European users etc. However, if service provider in Asia has only upstream connectivity to USA region considering other ISP link decision factors, users experience high latency to Asian destinations, hence low user experience. Therefore, Internet service providers are responsible for setting up multiple upstream connections to different geographic regions of the world.

Setting-up upstream connections are influenced by different factors such as cost, capacity, and access to global intent connectivity through undersea internet cables. Setting-up multiple upstream internet connections do not guarantee that all latency issues will be resolved. Even though multiple upstream connections are available to different locations, packet data transfer path selection depends on routing protocol used and Internet connectivity topology. BGP is the protocol that ISPs use to exchange routing information between autonomous systems. End of this chapter describes how

BGP protocol selects the best path when multiple paths are available to a particular destination, using graphical diagrams.

1.3 Boarder Gateway Protocol (BGP)

When the Internet grew and moved to Autonomous System (AS) architecture, EGP was still able to function as the exterior routing protocol for the Internet. However, as the number of autonomous systems in an internetwork grows, the importance of communication between them grows as well. EGP was functional but had several weaknesses that became more problematic as the Internet grew in size. It was necessary to define a new exterior routing protocol that would provide enhanced capabilities for use on the growing Internet. In June 1989, the first version of this new routing protocol was formalized, with the publishing of RFC 1105, a Border Gateway Protocol (BGP). This initial version of the BGP standard defined most concepts behind the protocol, and the key fundamentals such as messaging, message formats, and how devices operate in general terms. It established BGP as the Internet's exterior routing protocol of the future. In 1994, BGP-4 was introduced with more capabilities and RFC 4271 is the latest RFC.

In today’s context, BGP is the one and only protocol used by ISPs to exchange routing information between Autonomous numbers. An Autonomous System is a network or group of networks under a common administration and with common routing policies. BGP helps to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). Customer networks such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as RIP or OSPF to exchange routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

BGP is distance vector protocol. BGP protocol does not consider geographic distance to destination and outgoing interface congestion status when selecting best route to the destination. BGP uses TCP port 179 to exchange information between neighbors. Every BGP speaking router receives reachability information from its neighbors, it then chooses the best route based on predefined set of rules. In most cases, BGP protocol selects the shortest AS-Path unless special policy has been configured to influence the route selection.

AS-Path is the list of AS numbers between source and destination. With BGP, it is not necessary to refresh routing information as with many other routing protocols. Instead, when a router advertises a prefix to one of its BGP neighbors, that information is considered valid until the first router explicitly advertises that the information is no longer valid or until the BGP session itself is lost or closed. There are four possible message types used with BGP; OPEN, UPDATE, NORTIFICATION, and KEEP_ALIVE.

1.4 ISPs Upstream Connectivity

Figure 3 presents a typical autonomous system interconnect scenario around the world to achieve global connectivity.

Figure 3: Typical ASN interconnect Scenario

Figure 4 illustrates Sri Lanka Telecom, the largest internet service provider in Sri Lanka, achieves global connectivity as at 2015 November with multiple upstream connections. Sri Lanka Telecom has ten IPV4 upstream connections and 9 IPV6 upstream connections to achieve global connectivity.

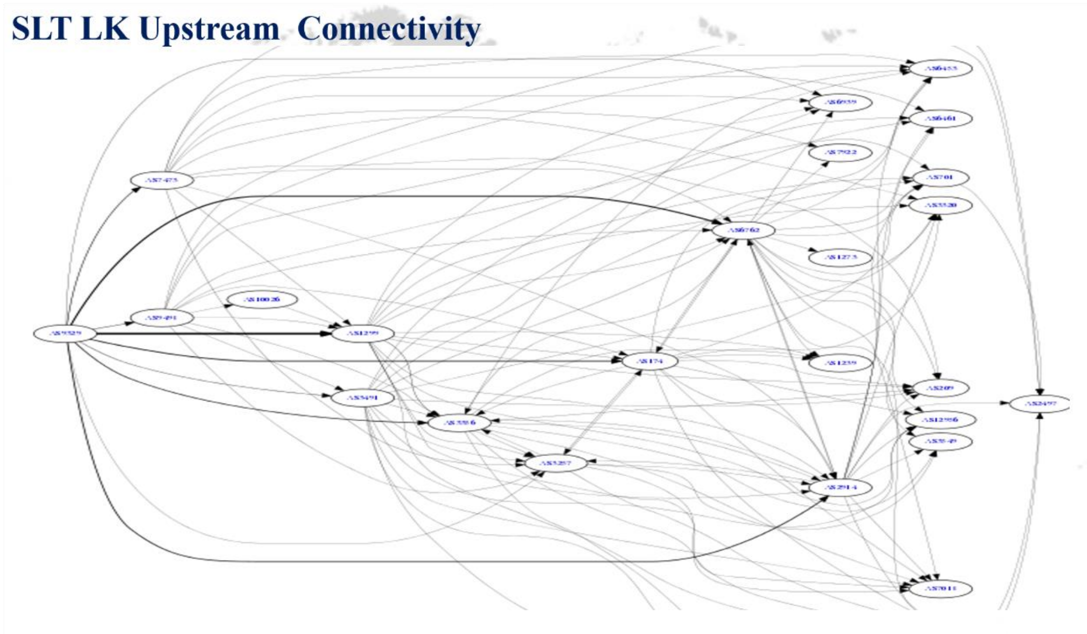

Figure 4: How Sri Lanka Telecom connects to upstream ISPs

Figure 5 illustrates how Dialog Axiata, one of the mobile and fixed broadband service providers of Sri Lanka, achieves its global internet connectivity as at 2015 November with multiple upstream connections. Dialog Axiata has seven IPV4 upstream connections and five IPV6 upstream connections to achieve global connectivity.

Figure 6 demonstrate how Sri Lanka Telecom Mobitel, one of the mobile broadband service providers of Sri Lanka, achieves its global internet connectivity as at 2015 November with multiple upstream connections. Sri Lanka Telecom Mobitel has four IPV4 upstream connections and two IPV6 upstream connections to achieve global connectivity.

Figure 4, Figure 5, and Figure 6 confirm internet service providers have multiple upstream ISP connections. This is to achieve reliable connectivity and reach global destinations with shortest distance.

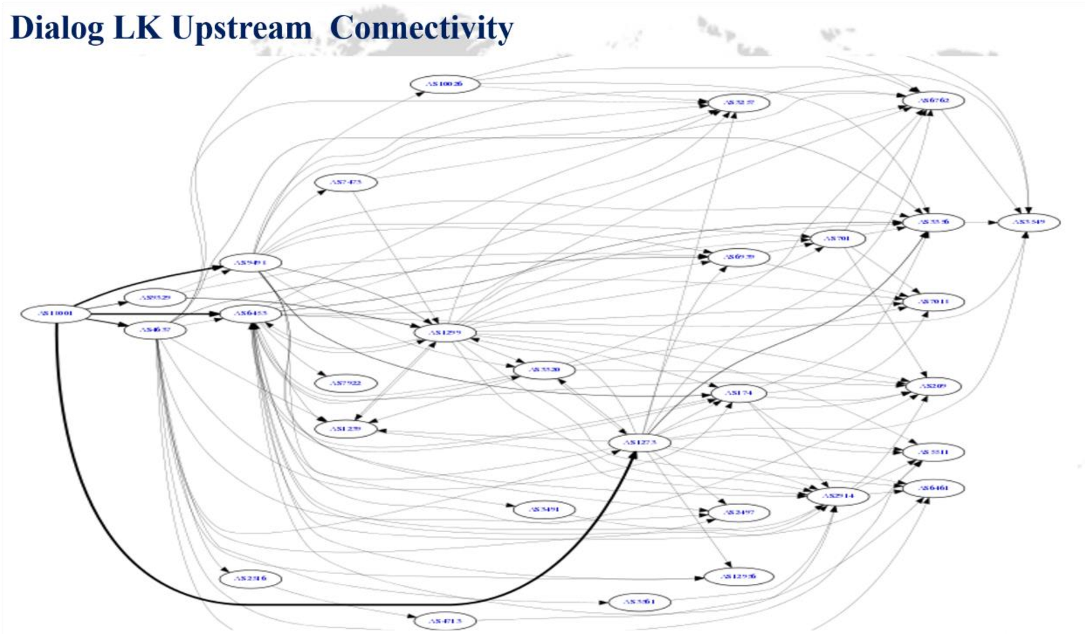

Figure 5: How Dialog Axiata connects to upstream ISPs

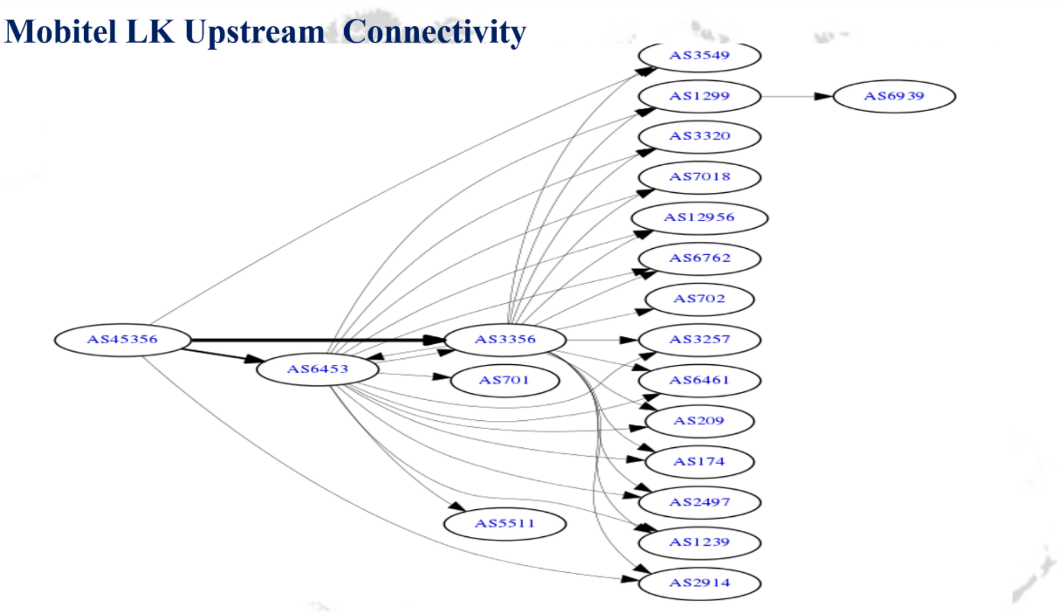

Figure 6: How SLT Mobitel connects to upstream ISPs

1.5 BGP Route Selection Possibilities

Figure 7, Figure 8, and Figure 9 provide three scenarios of how BGP protocol select best path to reach destination when multiple upstream connections exits and no route policy applied.

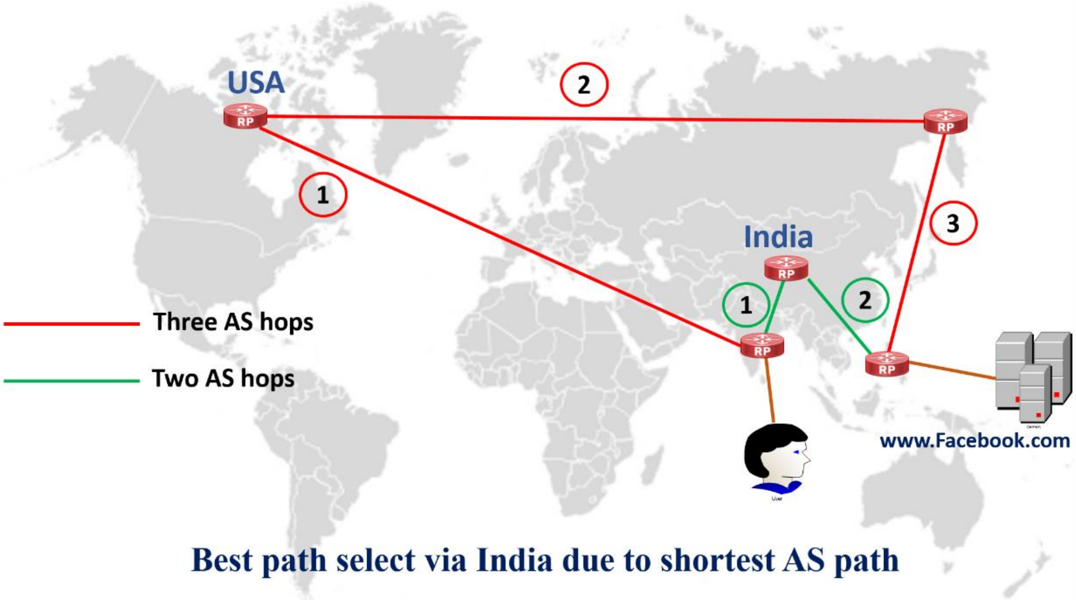

Figure 7: BGP best path selection scenario - 1

According to Figure 7, if user attempts to reach www.facebook.com server hosted at Singapore data center from Sri Lanka, BGP selects best IP path via India since IP path via India has two AS hops. There are three AS hops via USA.

According to Figure 8, if user tries to reach www.facebook.com server hosted at Singapore data center from Sri Lanka, BGP selects best IP path via USA since IP path via USA has two AS hops. There are three AS hops via India and it will not be the best path even through it is the shortest distance, hence shortest latency path. However, this is not the best path selection and it will create high latency to the destination.

According to Figure 9, if user aims to reach www.facebook.com server hosted at Singapore data center from Sri Lanka, BGP selects best IP path randomly based on predefine conditions since both paths have similar AS path lengths.

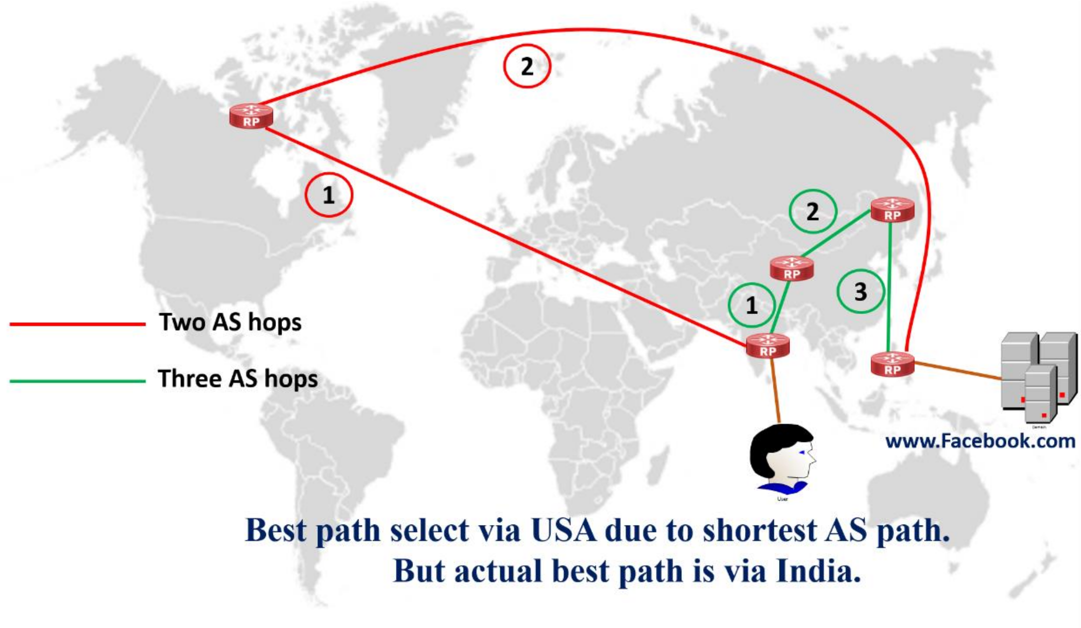

Figure 8: BGP best path selection scenario – II

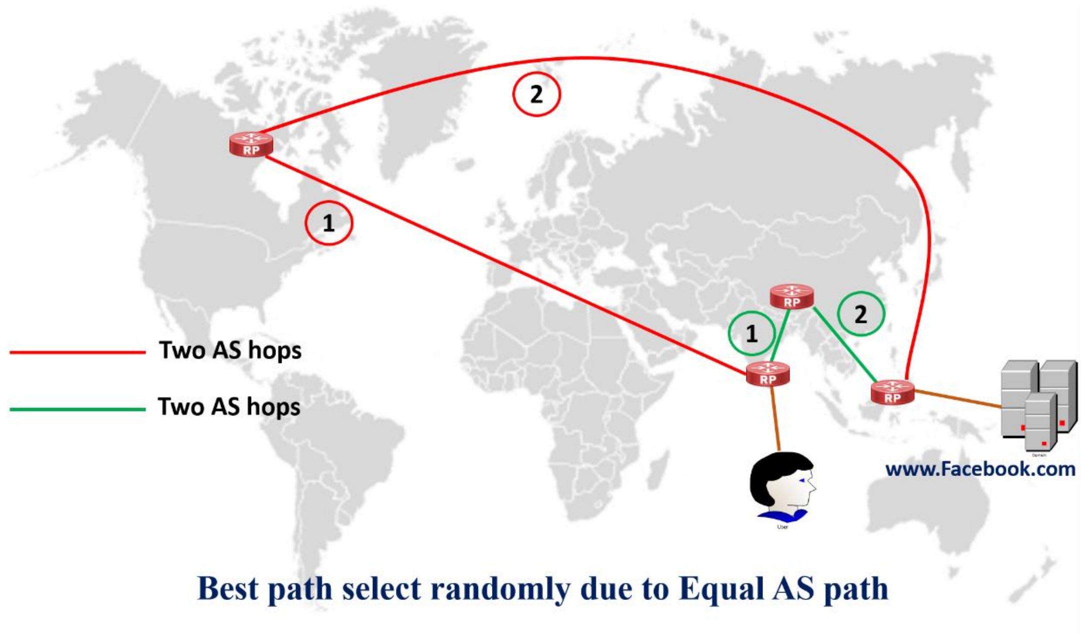

Figure 9: BGP best path selection scenario – III

The scenario described in Figure 9 motivates this research. One purpose of this research is to analyses current BGP full routing table in ISP multi-homing environment and check percentage of routes with equal AS-PATH lengths similar to scenario described in Figure 9. Equal AS-PATH length results BGP protocol to select outgoing interface randomly based on lowest router ID or lowest interface ID. This may result high latency and thus low Quality of Service. Therefore, this proposal suggests new route selection criteria when router meets equal length AS paths.

1.6 Motivation and Objective

Most prevailing issue for South Asian internet users is that Internet content is not hosted within the region, but in Singapore, Europe, and USA data centers. It is a well-known phenomena that Top content providers try to serve South Asian users from Singapore based data centers due to shortest physical distance. BGP protocol does not select shortest distance path always when multiple upstream connections are available to ISP. This results in high latency to end users. BGP protocol may consider path to reach Sri Lanka from Singapore data center via USA despite the direct IP path between Singapore and Sri Lanka. In such a situation, end users experience high latency if BGP protocol selects incorrect path to destination. From South Asian internet users' point of view, this is a critical issue. However, this is not a critical issue from Europe and USA internet users' point of view since they have content within their region. This is the basic criteria motivated this research.

One purpose of this research is to analyze current BGP full routing table in ISP multi-homing environment and check percentage of routes with equal AS-PATH length. Equal AS-PATH length results BGP protocol to select outgoing interface randomly based on lowest router ID or lowest interface ID. This may result in high latency and thus low Quality of Service. Another objective is to suggest new route selection criteria when router meets equal length AS paths.

Simulation results reveal nearly 50 percent routing decisions are based on equal AS-PATH length if special routing policies are not applied. Further, simulation result justifies a relationship between latency and web page browsing user experience. Therefore, geographic location based route selection for BGP protocol when AS-PATH length is equal is proposed in this research paper.

1.7 Organization of the Thesis

In this thesis, focus is made on three aspects of the BGP protocol. One aspect is to analyze existing BGP routing table and find out how many routes have equal BGP AS-PATH length when there is no routing policy configured. Second aspect is to find out any relationship between latency and end user experience. Time taken to load web page with different latency values has been considered as user experience. Finally, possible solutions to reduce latency in ISP environment and implementation suggestion are discussed.

Chapter 2 describes exiting literature on Boarder Gateway Protocol and internet routing. Chapter 3 explains the proposed methodology. Expected results are discussed in Chapter 4. Chapter 5 discusses SDN implementation possibility and the conclusion and future work are described in Chapter 6.

Chapter 2

LITERATURE REVIEW

2.1 Internet Connectivity Topology

The Internet forms by connecting collections of internet service providers (ISP). Each ISP is uniquely identified by Autonomous System number (AS) and each AS is assigned with unique IP address pools to communicate between ASs. IETF defines autonomous systems as a set of routers under a single technical administration, using an interior gateway protocol (IGP) and common metrics to determine how to route packets within the AS, and using an inter-AS routing protocol to determine how to route packets to other AS. Since this classic definition was developed, it has become common for a single AS to use several IGPs and, sometimes, several sets of metrics within an AS. Use of the term Autonomous System stresses the fact that, even when multiple IGPs and metrics are used, the administration of an AS appears to other AS to have a single coherent interior routing plan, and presents a consistent picture of destinations that are reachable through it [2]. Figure 3 provides a typical connection scenario of ISPs. One ISP can have single or multiple upstream connections. End users need to connect any of the Internet service provider in order to access any internet based service. Similarly, internet based service providers need to connect any ISP, anywhere in the world.

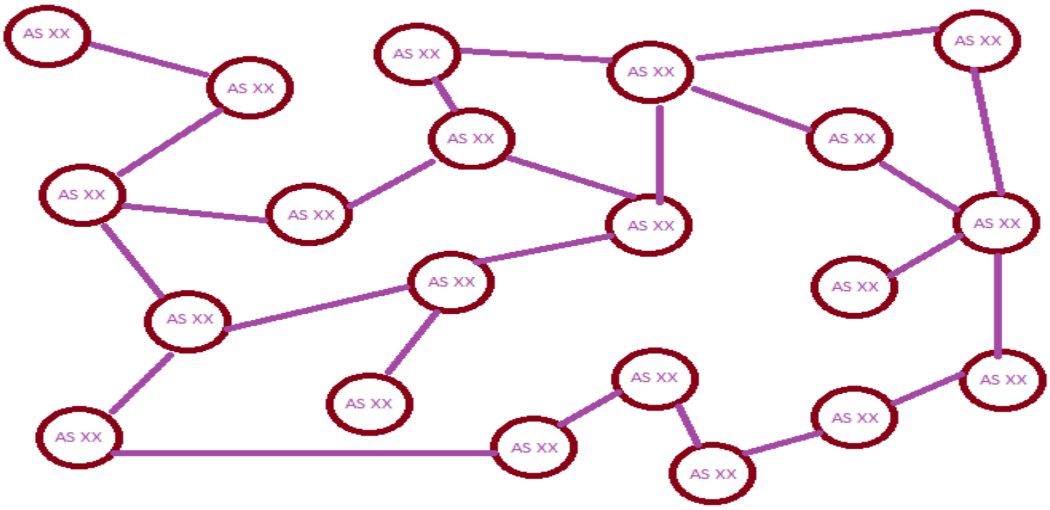

Figure 10: ISP Connectivity

These Internet service providers (AS XX) provide services such as internet access, internet transit services, domain name registration, web hosting, caching and content filtering, and network threat detection and prevention. In the past, most Internet service providers were telecommunication companies. However, there are several non-telecom ISP providers nowadays and currently it is becoming a new business opportunity. Internet service providers provide different technologies to connect end users. ADSL, DSL, Metro Ethernet, Carrier Ethernet, Ethernet, Gigabit Ethernet, and Wireless connectivity are some of the end user technologies provided by ISPs. End users need to connect or get service from any destination of the Internet. To achieve this, end users need to purchase service from their Internet service providers using any of the above-mentioned technologies. Normally this is a paid connection and ISPs provide such service based on link speed, monthly usage etc. Internet service providers need to connect all other Internet service providers to achieve global connectivity. Creating full mesh network among each ISPs is not practical in today context. However, logical full mesh connectivity to achieve global reachability irrespective of geographic locations is a requirement. ISPs achieve this requirement through concept call peering, transit, and using routing protocols. Peering defines interconnection of administratively separate Internet networks for exchanging traffic between the users of each network. There are two types of peering; private peering and public peering. Public peering, also known as IPX, is achieved though layer 2 connectivity and multiple carries interconnect with one or multiple carriers at single port

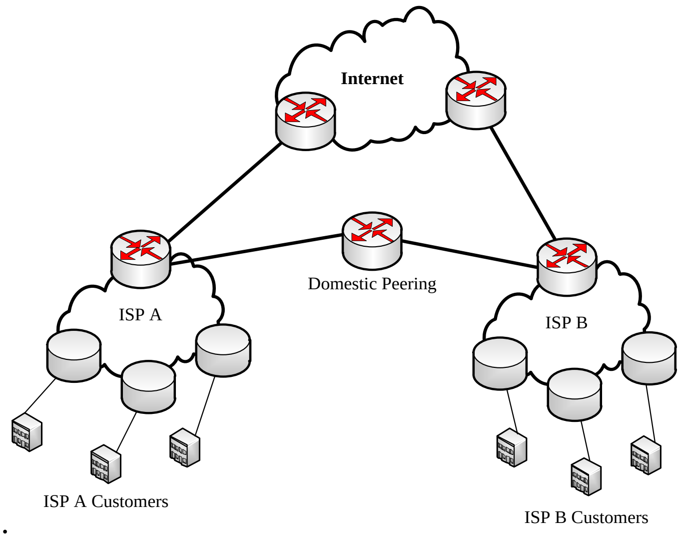

Figure 11: Illustration of IXP peering

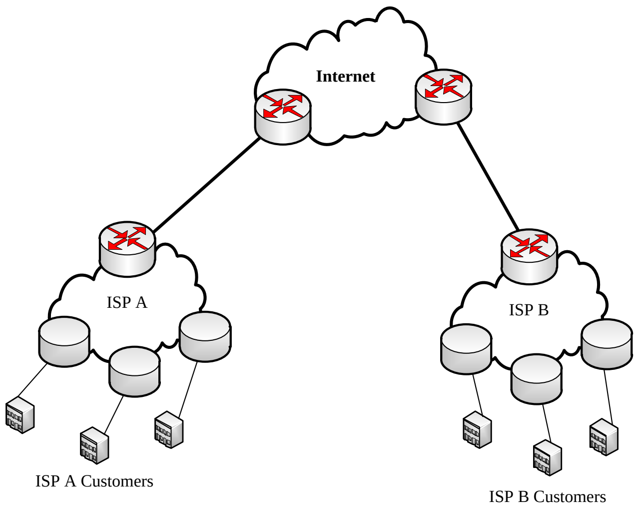

Figure 12: Illustration of direct peering without IXP

The primary role of an IXP is to keep local Internet traffic within local infrastructure and to reduce costs associated with traffic exchange between Internet Service Providers (ISPs). IXPs allow for the free exchange, or peering, of domestic Internet traffic between Internet service Providers (ISPs). Within the Internet community, IXPs are considered to facilitate Internet-based economic growth. The absence of IXPs compromises our ability to build a robust domestic Internet ecosystem and economy [3]. Another role of IXP is to improve latency to destination. In this setup, multiple number of ISPs connects to same physical location having aim of exchanging user traffic. Therefore bandwidth is shared among each other and there is no dedicated bandwidth assigned to individual ISPs. Even though IPX are initially setup in order to route domestic traffic locally some ISPs get IXP service from regional IXPs. This is to reduce latency and get cost advantage over private peering.

Private peering is the direct interconnection between two ISPs using layer 1 or layer 2 technology. In private peering, dedicated bandwidth is assured and cost is very high. Current private peering occurs 10Gbps capacity level and still operators use STM1 (~ 155 Mbps), STM4 (~ 600Mbps), STM16 (~ 2.4 Gbps), or multiple of 1Gbps links through private peering. Small ISPs tend to peer with IXPs instead of private peering if they have cost concerns on private peering. Other interconnect method is called Transit. In transit scenario, one ISP is paid to upstream ISP for the internet service. In peer mode peers exchange traffic among each other with no cost to each other for mutual benefits. Typically, transit is the most expensive mode of interconnection. ISPs are ranked based on its interconnection topology. Tier 1 can be defined as networks that do not pay any other network for transit, however still can reach all networks connected to the internet. Tier 2 networks can define as networks that peer with some networks and purchases IP transit or pay settlements from some of ISPs. A network that solely purchases transit from other networks to access internet is called tier 3 network. Figure 6 illustrates typical architecture of ISPs connectivity.

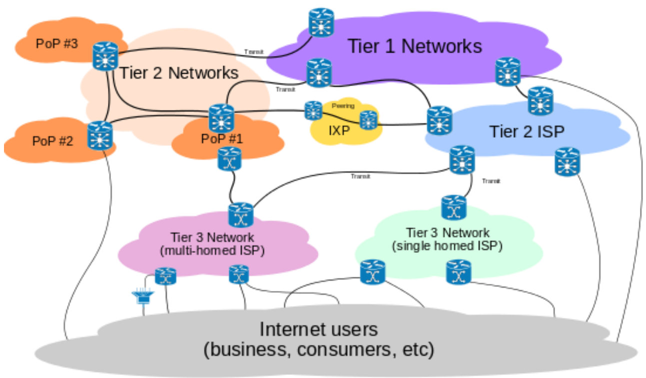

Figure 13: Type of ISP

Source: https://en.wikipedia.org/wiki/Tier_1_network

Above section clearly describes the internet and the way Internet service providers connect each other to achieve global connectivity. Physical connectivity alone does not make internet works, but there should be a mechanism to route packets among ISPs. Next chapter discuss how packet route in internet efficiently.

2.2 Internet Routing

As described in previous chapter, internet service providers are uniquely identified by AS number in internet routing domain. The Border Gateway Protocol version 4 (BGP) is the *de facto* inter-domain routing protocol presently used in the Internet. BGP is a policy-based, path-vector protocol that distributes route information between Autonomous Systems (AS) [2]. According to RFC 4271, the primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASs) that reachability information traverses. This information is sufficient for constructing a graph of AS connectivity for this reachability, from which routing loops may be pruned and, at the AS level, some policy decisions may be enforced. Further, in RFC 4271, it is mentioned that routing information exchanged via BGP supports only the destination-based forwarding paradigm, which assumes that a router forwards a packet based solely on the destination address carried in the IP header of the packet. This in turn reflects the set of policy decisions that can (and cannot) be enforced using BGP. BGP can support only the policies conforming to the destination-based forwarding paradigm. BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing.

2.2.1 BGP Protocol

In order to make suggestion or improvement to BGP protocol, there should be good knowledge about protocol, its message format, and operation. BGP listens on TCP port 179. There are four types of messages in BGP protocol; Open, Update, Notification, and Keep alive. Initially, BGP speakers setting up TCP connection over port 179. After a TCP connection is established, the first message sent by each side is an OPEN message. If the OPEN message is acceptable, a KEEPALIVE message sends confirming the OPEN is sent back. OPEN message includes BGP version number, AS number, hold time, BGP identifier, and optional parameters. Following figure presents the BGP open message format.

2.2.2 Message Types and Format

2.2.2.1 Open Message

<table>
<tr><td colspan="3">32 bits</td></tr>
<tr><td colspan="2"></td><td>Version (1 byte)</td></tr>
<tr><td colspan="2">My Autonomous System (2 bytes)</td><td>Hold Time (2 Bytes)</td></tr>
<tr><td colspan="3">BGP Identifier (4 Bytes)</td></tr>
<tr><td>Opt Param Len
(1 byte)</td><td colspan="2">Optional Parameters (Variable Length)</td></tr>
</table>

Figure 14: BGP Open Message Format

Source: http://www.itcertnotes.com/2012/01/bgp-message-types.html

***Version*:** A 1-byte field that indicates the BGP version number running on the originator. The highest common version that both routers negotiated and support is used. Most current BGP implementations use the current version – BGP-4 [4].

My Autonomous System: A 2-byte field that indicates the AS number of the originator. A BGP peer uses this information to determine whether the BGP session is EBGP or IBGP and will terminate the BGP session if it is not the expected AS number.

Hold Time: A 2-byte field that indicates the number of seconds proposed by the originator for the hold time of the BGP session – the time period that can elapse before the receiver must receive either a keepalive or Update message from the originator. The receiver of the Open message calculates the hold timer value to use by comparing the Hold Time field specified in the Open message and its configured hold timer value, and accepts a smaller value or rejects the connection. The hold time must be either 0 or at least 3 seconds, and the default hold time is 180 seconds.

BGP Identifier: A 4-byte field that indicates the Router ID of the originator. The BGP identifier is an IP address assigned to a BGP router and is determined upon the startup of a BGP routing process. The BGP Router ID is chosen the same way as the OSPF Router ID is selected. The BGP Router ID can be configured statically to override the automatic selection.

Optional Parameters Length: A 1-byte field that indicates total length of the following Optional Parameters field, in octets. A value of zero indicates no Optional Parameters field is included in the Open message.

Optional Parameters**:** A variable-length field that contains a list of optional parameters. Each parameter is specified by a 1-byte Type field, a 1-byte Length field, and a variable-length Value field that contains the parameter value itself. This field is used to advertise the support for optional capabilities such as multiprotocol extensions, route refresh, etc.

2.2.2.2 Update Message

The update message lists withdrawn and new routes. Figure 15 specifies UPDATE message format.

Unfeasible routes Length (2 bytes)		**Unreachabel Routes**
Withdrawn Routes (variable - length)		
Total Path attribute Length (2 bytes)		**Path Attributes**
Path Attributes (Variable Length)		
Length (1 byte)	**Prefix** (1/2/3/4 bytes)	**Network Layer Reachability Information (NLRI)** (variable Length)
Length (1 byte)	**Prefix** (1/2/3/4 bytes)	
Length (1 byte)	**Prefix** (1/2/3/4 bytes)	

Figure 15: BGP Update Message Format

Unfeasible Routes Length: A 2-byte field indicating total length of the following Withdrawn Routes field in octets. A value of zero indicates that no routes are withdrawn and there is no Withdrawn Routes field included in the Update message.

***Withdrawn Routes*:** A variable-length field that contains a list of unreachable routes that are to be withdrawn from service, if any. Each route in the list is described with a (Length – Prefix) tuple. If the Length part of the tuple is 0, the Prefix matches all routes.

Total Path Attribute Length: A 2-byte field that indicates total length of the following Path Attributes field, in octets.

Path Attributes: A variable-length field that lists the attributes associated with the NLRI in the following field. Figure 9 shows detail on Path attribute field.

2.2.2.3 Path attribute

2 byte

O	T	P	E	U	U	U	U	Attribute Type Code (1 byte)

Flag Bits

O – Optional Bit

0 - Well-known

1 – Optional

T – Transitive Bit

0 – None-Transitive

1 – Transitive

P – Partial Bit

0 – Optional Transitive Attribute is complete

1 – Optional Transitive Attribute is partial

E – Extended Length Bit

0 – The Attribute Length is 1 Byte/Octet (Regular Length)

1 – The attribute Length is 2 Bytes/Octet (Extended Length)

U – Unused Set to 0

Attribute Type Code	Attribute Type	Class	Attribute Value code	Attribute Value
1	ORIGIN	Well-known mandatory	0	IGP
			1	EGP
			2	Incomplete
2	AS_PATH	Well-known mandatory	1	AS_SET
			2	AS_SEQUENCE
			3	AS_CONFEED_SET
			4	AS_CONFEED_SEQUENCE
3	NEXT_HOP	Well-known mandatory	0	Next-Hop IP address
4	MULTI_EXIT_DISC	Optional non-transitive	0	4 byte MED
5	LOCAL_PREF	Well-known mandatory	0	4 byte Local_PREF
6	ATOMIC_AGGREGATE	Well-known mandatory	0	None
7	AGGREGATOR	Optional non-transitive	0	ASN and IP Address of Aggregator
8	COMMUNITY	Optional non-transitive	0	4- octet Community Identifier

9	ORIGINATOR_ID	Optional non-transitive	0	4 – Octet Router ID of Originator
10	CLUSTER_LIST	Optional non-transitive	0	Variable-Length List of Cluster IDs

Figure 16: Path attribute header format

Network Layer Reachability Information (NLRI): A variable-length field that contains a list of IP prefixes that can be reached via this path using the (Length – Prefix) tuples. A Length value of 0 indicates a prefix that matches all IP prefixes.

2.2.2.4 Keepalive and Notification Message

Keepalive messages are transmitted when the connection is idle, to make sure hold timer does not expire. Type field is set to 4 when message type is keep alive. A notification message is generated when a fetal error condition arise. The sender tears down the TCP connection after sending notification message to peer. Figure 17 shows message format of keepalive and notification.

32 buts		
Marker (16 bytes)		
Length (2 bytes)	Type (1 byte)	

Figure 17: BGP Keepalive and Notification message format

Notification**:** Type Code used for notification message is 3.
Keepalive**:** Type Code used for keepalive message is 4.

2.2.3 BGP Best Path Selection

Most internet service providers use more than one upstream connections to achieve redundancy and best quality of service. Obviously one reason is to achieve best latency to remote destination. As described in previous chapters, BGP is the only one protocol used by ISPs current context. Thus, BGP needs a mechanism to select best route from the set of available routes from different neighbors. For this purpose, several attributes are communicated from the BGP speakers to the next speaker. Those attributes are called as path attributes and send using BGP update message. Following are types of path attributes used by BGP protocol.

Well-known mandatory: All BGP routers present in all BGP updates must recognize this type of path attributes and passed on to other BGP routers; i.e. AS path, origin, and next hop.

Well-known discretionary: All BGP routers must recognize this type of path attributes and passed on to other BGP routers, but need not be present in an update; i.e. local preference.

Optional transitive: This type of path attributes 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 no transitive: This type of path attribute 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.

2.2.4 Path Selection Attributes

Following describes path attributes, which belong to one of the above types.

Local preference

The local preference is a value local to an AS communicated over the intra-AS BGP sessions. BGP always prefer to route with highest local preference.

AS Path

The AS path lists all the AS numbers between the local router and the source of the route. This includes the source AS number for none local routs but not the local AS number. The path is used for several purposes. First, it prevent routing loop. A router ignore ant routes it receives from a router in a neighboring AS that contain its own AS number.AS path enables routers to make a policy decision based on preference of certain ASs in the path. BGP RFC specifies routes with shorter AS path and are preferred over routers with a longer AS path.

Next hop

The next hop attribute contains the IP address of the router within the remote AS that will accept packets for the current route.

MED

The multi exit discriminator (MED) was designed to give a neighboring AS about which connection is preferred when there are multiple connections between ASs.

Origin

This attribute conveys source for the BGP announcement, an IGP, the EGP protocol, or the other means.

Communities

A route may contain one or more communities. A community is of 32-bit value and often expressed in a form such as XXX: YYY. XXX is AS number and YYY is a value that has meaning within AS XXX.

2.2.5 Standard BGP Path Selection Algorithm

BGP protocol uses following sequence when deciding best route based on above described attributes.

1. Discarding routes with the unreachable Next_Hop.
2. Preferring route with the highest Local_Pref.
3. Preferring the aggregated route. The preference of an aggregated route is higher than the preference of a non-aggregated route.

4. Preferring the route with the shortest AS-Path.
5. Comparing the Origin attribute and selecting the routes with the Origin attribute as IGP, EGP, or Incomplete in order.
6. Preferring the route with the smallest MED value.
7. Preferring the route learned from EBGP. The preference of an EBGP route is higher than that of an IBPG route.
8. Preferring the route with the smallest IGP metric in an AS. Load balancing is performed according to the number of configured routes if load balancing is configured and there are multiple external routes with the same AS-Path.
9. Preferring the route with the shortest Cluster List.
10. Preferring the route with the smallest Originator ID.
11. Preferring the route advertised by the router with the smallest router ID.
12. Comparing IP addresses of the peers and preferring the route that is learnt from the peer with a smaller IP address.

BGP protocol select best route based on above 12 steps. According to above steps, if a route does not set local preference manually, AS path length is the dominant selection criteria. If routes receives a same route with equal AS path length, then router go for the next option. Most possible selection criterion is the smallest originator ID.

2.2.6 Route Policy and BGP Community Strings

During the early days of the Internet, the problem of how to route packets to their final destination was much simpler than it is today. When BGP was first introduced, it was a simple path vector protocol. Over time, many incremental modifications to allow ISPs to control routing were proposed and added to BGP. The end result was a protocol weighted down with a many number of mechanisms that can overlap and conflict in various unpredictable ways. These modifications can be highly mysterious since many of them, including the decision process used to select routes, are not part of the protocol specification. Moreover, their complexity gives rise to several key problems, including unforeseen security vulnerabilities, widespread misconfiguration, and conflicts between policies at different ISPs [5].

BGP Routing policy plays a major role in above explanation. When Internet grows, complex routing requirements arise and it is hard to change traditional BGP protocol due to popularity of the BG protocol, and most routers being used BGP in production environment. Thus, most routing decisions changed though BGP route policies and BGP community strings. The primary task of the BGP route policy is to change any of the parameter values used for best route selection described in previous chapter. For example, router may change local preference values of routes originated from BGP peer IP xx whose origination is marked as Europe region though BGP community strings. Then router route traffic belongs to Europe through specific interface. However, this capability is purely depends on upstream ISP traffic marking and local router routing policy.

Most of tier 1 ISPs mark route origination using BGP community strings and definitions of such community strings are local to ISP. In most cases, route origination is marked up to regional level. For example North America, South America, Europe, Asia etc.

US MSA origins (2914:10--)

2914:1001	Ashburn, VA
2914:1001	Sterling, VA
2914:1002	Atlanta, GA
2914:1003	Chicago, IL
2914:1004	Dallas, TX
2914:1004	Houston, TX
2914:1005	Los Angeles, CA
2914:1006	Miami, FL
2914:1007	Seattle, WA
2914:1008	Milpitas, CA
2914:1008	Mountain View, CA
2914:1008	Palo Alto, CA
2914:1008	San Jose, CA
2914:1008	Santa Clara, CA
2914:1009	New York, NY
2914:1010	Sacramento, CA

Figure 18: AS 2914 BGP community marking based on route originate location

Source: http://www.us.ntt.net/support/policy/routing.cfm

Some of ISPs make router origination up to country level but not for all countries. Below figure presents how NTT (AS 2914) mark traffic based on route origination.

Local routers can apply route policy based on above definitions. For example, local router administrator can change local preference value of routes originated from Seattle, WA, by machining BGP community string 2914:1007. It is explained in previous chapter that BGP protocol selects best route with highest local preference value. However, above BGP community strings are not unique and therefore local route configuration is not unique.

2.3 BGP Route Selection Possibilities

2.3.1 Unequal Path

Purpose of this research is to suggest new route selection criterion based on geo location of route originate for BGP protocol. It is required to get a better understanding how BGP protocol currently route traffic in the Internet through an example. Figure 19 shows two different scenarios when traffic passes from AS-0 to point AS-6.

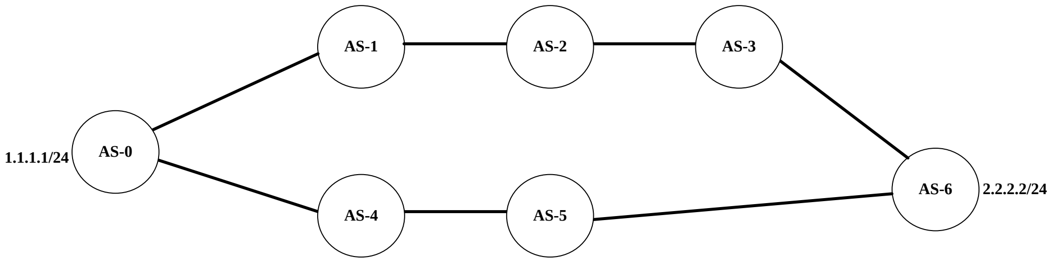

Figure 19: BGP route Selection Unequal Path

Assume in Figure 19 end users of AS_0 need to visit web page hosted at AS-6. End customer who belong IP address 1.1.1.1 can connect to its local ISP though any means of media described in Chapter 1 of this paper. It could be DSL, ADSL, Ethernet or wireless or whatever access technology. AS-0 to AS-6 located different geographic region of the world map. For example, AS-0 can be in Sri Lanka and AS-6 can be in United States of America. AS-2 could be Europe and As5 can be Singapore. AS-0 need to connect ISP cloud in to achieve global reachability. In this scenario AS-0 has two upstream connectivity to achieve global reachability; through AS-1 and AS-4. Similarly, web server which AS-0 customer need to connect has been hosted under ISP AS-6 and AS-6 has two upstream connectivity to achieve global reachability. Only possible protocol runs between, AS is BGP. Thus, AS-0 to AS-6 run BGP protocol and advertise route each other to make global reachability. We assume there is no capacity limitation between AS-0 to AS-1 and AS-4. Similarly, we assume there is no capacity limitation between AS-6 to AS-3 and AS-5. If we check BGP routing table at AS-6, it should provide something similar to below illustration.

Network	**Next-hop**	**MED**	**Local Pref**	**Path/Origin**
1.1.1.0/24	Though AS-3	0	100	AS-3, AS-2, AS-1, AS-0 **i**
	Though AS-5	0	100	AS-5, AS-4, AS-0 **i**

When BGP protocol selects best route to reach IP network 1.1.1.0/24, it follows logic described in previous chapter under best path selection and select best route based best matching criteria. In this scenario LF and MED is equal and preference is done based on AS path length. Thus AS-6 selects path though AS-5 to reach AS-0 network since length is 3.

Similarly, we can describe how AS-0 select to reach AS-6. Below figure illustrate AS-0 BGP routing table.

Network	**Next-hop**	**MED**	**Local Pref**	**Path/Origin**
2.2.2.0/24	Though AS-1	0	100	AS-1, AS-2, AS-3, AS-6
	Though AS-4	0	100	AS-4, AS-5, AS-6i

When BGP protocol selects best route to reach IP network 2.2.2.0/24, it follows logic described in previous chapter under best path selection and selects best route based on best matching criteria. Within this context LF and MED is equal and preference based on AS path length. Thus, AS-0 selects path though AS-4 to reach AS-0 network since length is 3.

Based on above explanation, AS-0 selects AS-4 to reach AS-6 and AS-6 selects AS-5 to reach AS-0. After this routing selection, end users at AS-0 can reach web server hosted at AS-6.

When the scenario in figure 20 is discussed, AS connectivity is different from previous scenario described.

2.3.2 Equal Path

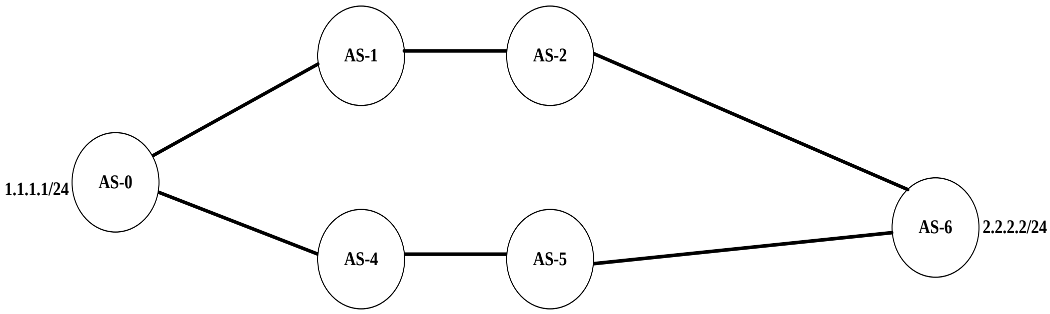

Figure 20: BGP route Selection Equal Path

Assume in Figure 20, end users of AS_0 need to visit web page hosted at AS-6. End customer who belonging IP address 1.1.1.1 can connect to its local ISP though any means of media described in Chapter 1 of this paper. It could be DSL, ADSL, Ethernet or wireless or whatever access technology. AS-0 to AS-6 are located in different geographic region of the world map. For example, AS-0 can be in Sri Lanka and AS-6 can be in United States of America. AS-2 could be Europe and As5 can be Singapore. AS-0 needs to connect ISP cloud in to achieve global reachability. In this scenario AS-0 has two upstream connectivity to achieve global reachability; through AS-1 and AS-4. Similarly, web server, which AS-0 customer need to connect has been hosted under ISP AS-6 and AS-6 has two upstream connectivity to achieve global reachability. Only possible protocol runs between, AS is BGP. Thus, AS-0 to AS-6 run BGP protocol and advertise route each other in order to make global reachability. We assume there is no capacity limitation between AS-0 to AS-1 and AS-4. Similarly, we assume there is no capacity limitation between AS-6 to AS-3 and AS-5. If we check BGP routing table at AS-6, it should reveal something similar to below illustration.

Network	**Next-hop**	**MED**	**Local Pref**	**Path/Origin**
1.1.1.0/24	Though AS-2	0	100	AS-2, AS-1, AS-0 **i**
	Though AS-5	0	100	AS-5, AS-4, AS-0 **i**

When BGP protocol selects best route to reach IP network 1.1.1.0/24, it follows logic described in previous chapter under best path selection and selects best route based on best matching criteria. In this scenario LF and MED are equal and next selection criteria is AS path. However, in this case, AS path length is equal and route operation systems need to check for other criteria. Thus AS-6 may select a path though AS-2 to reach AS-0 network based on local router ID. Here whether router has selected best path since both path shows equal to BGP logic, is unknown.

Similarly we can describe how AS-0 select to reach AS-6. Below figure illustrate AS-0 BGP routing table.

Network	**Next-hop**	**MED**	**Local Pref**	**Path/Origin**
2.2.2.0/24	Though AS-1	0	100	AS-1, AS-2, AS-6 i
	Though AS-4	0	100	AS-4, AS-5, AS-6 i

When BGP protocol selects best route to reach IP network 2.2.2.0/24, it follows logic described in previous chapter under best path selection and selects best route based best matching criteria, Here, LF and MED are equal and next selection criteria is AS path. However, in this case, AS path length is equal and route operating systems needs to check for other criteria. Thus, AS-0 may select a path though AS-4 to reach AS-6 network based on local router ID (or some other criteria). Here, we do not know whether router has selected best path since both path shows equal to BGP logic.

Based on the above explanation, AS-0 selects AS-4 to reach AS-6 and AS-6 selects AS-2 to reach AS-0. After this routing selection, end users at AS-0 can reach web server hosted at AS-6.

In both scenarios, AS-0 has reachability to AS-6 and AS-6 has reachability to AS-0. However, we are unaware whether route selects shortest path to reach destinations based on distance. Here it is very important to highlight that AS path length counts only hop count and not distance.

2.3.3 General scenario

Figure 21 provide a more general scenario where AS-0 has n number of upstream connections and AS-6 has n number of upstream ISP connections. AS-0 connects to AS-a1 to AS-an to achieve global reachability whereas AS-6 connects AS-b1 to AS-bn to achieve global reachability. Theoretically AS-0 receives n number of paths to select the best route to reach particular destination. BGP protocol follows BGP best route selection procedure and select on path as best hop. Similarly AS-6 has n number of paths to select the best path to destination. BGP protocol follows BGP best route selection procedure and select on path as best hop.

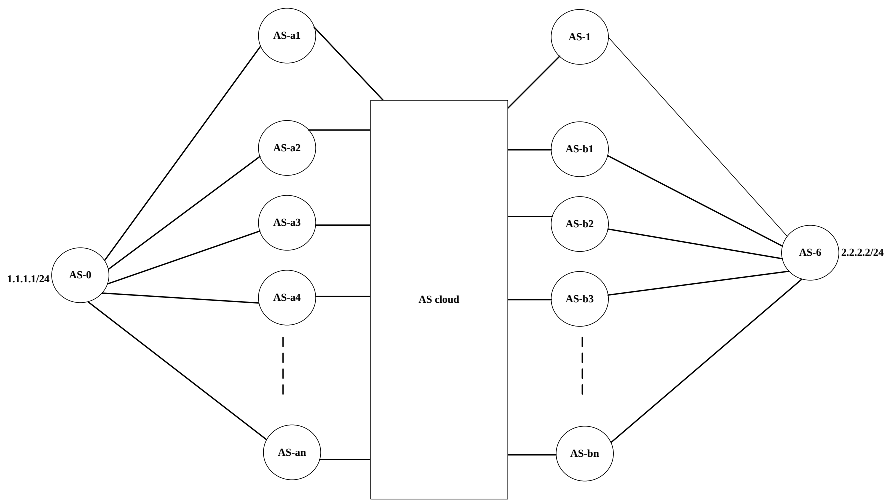

Figure 21: BGP route Selection General Case

2.4 Current Practices

2.4.1 Existing BGP Route Selection

Existing BGP route selection has been described clearly in previous section. Existing BGP protocol specifications do not take geo graphic distance to destination when selecting the best path. Currently the only protocol used on the Internet for the exchange of information between ISPs (Internet Services Provider) is known as BGP (Border Gateway Protocol [6]. A BGP router in an ISP may have several alternate routes to reach a particular destination. In the absence of policy, the router would choose the route with the minimum path length, with some arbitrary way to break ties between routes with the same path length [7]. BGP policies present a set of rules that define how an AS routes incoming and outgoing traffic to the Internet. In BGP, only one route is selected and advertised for each network destination prefix [8]. Multi-homing load balancing improves network performance by leveraging the traffic among the access links in a multi-homed network. Currently, no effective load balancing system is available to handle the inbound traffic in a BGP multi-homed stub network, where the traffic volume is unknown to the network and the route of the traffic is hard to control [9]. In the periphery of Internet, small ISP that usually gives services to enterprises that are not ISP. ISP can be classified as transit ISP when they offer transit of traffic, multi-homed ISP when they are connected to more than one ISP and do not offer transit of traffic and stub ISP when they are connected to only other ISP. An ISP can have more than one AS number assigned and give services to other ISP on large geographical areas [10]. Original BGP protocol only consider AS Path, Local preference, MED and Origin as parameters when selecting best route to a destination. Local Preference and MED effects only between immediate hop. There is no end-to-end visibility to above two parameters. Origin parameter has end-to-end visibility but there is no much practical importance of this parameter when route selection is considered. In most cases AS PATH length is the key best route selecting parameter in current context. This proposal shows that over 50 per cent of routes selected randomly due to match AP-PATH length.

BGP was first introduced in 1994 through RFC 1654, then RFC 771 in 1995, and the latest 1771 in 2006, followed by 6286, 6608, 6793(2012). There are several improvements from 1996 to 2012, but there is no change in under laying architecture on route selection. Many researchers have suggested several options to route selection with optional BGP parameters. BGP community strings are the most popular suggestions among them to influence the route selection. There is no universal standard for BGP community strings. Therefore community based route selection is depends on upstream community configuration. Millions of routes deployed in the world with BGP-4 support and entire Internet architecture depends on BGP-4 protocol. Therefore, it is very difficult to change core of BGP routing protocol. This could be the reason researchers do not work on core concept of BGP route selection criteria. However, quality of service is the key concern in today's context and software define network is becoming popular. Therefore, we can think changing core BGP route selection criteria will be available with SDN based routers.

Chapter 3

METHODOLOGY

In this paper, I have discussed present status of the Internet, Internet architecture and how routing happens within AS in the Internet. It was also mentioned that BGP is the only protocol currently used among ISP to route traffic between ASs.

Internet service provides setup multiple upstream connections to different geographic locations to achieve redundancy and best quality of service through low latency. However, setting up multiple upstream, connections only does not permit them to achieve better latency to a particular destination IP set. The path which data packets select to traverse from source AS to destination AS decide the time taken to reach destination. This time is known as latency. The purpose of this research is to check whether any relationship exists between latency and end user experience and if so, how to fine tune such relation by improving BGP protocol route selection criteria.

BGP is the only routing protocol that decides data packet transfer path between ASs. As described in previous chapters, BGP has pre-defined criteria to select outgoing path from particular router. Further, there are pre-define set of parameters in BGP protocol that helps to decide best outgoing path. The mechanism of population those parameters have been discussed in detail in this paper. When we analyze current BGP architecture and message format, it is clear that only one parameter is visible end-to-end. It is the AP path. All other parameters namely local preference, MED, Origin, and next hop are significant only between immediate BGP speakers. Therefore, if local router administrators do not influence local preference or MED value in BGP protocol, best path selection is most likely to base on AS path. The purpose of this research is to analyse current BGP routing table and check how many IP destinations have equal AS Paths. If equal AS PATH means router need to decide best outgoing path based on lowest router-ID or lowest interface IP. This does not guarantee the selection of best route by router to reach a particular destination. Two BPG routing tables have been considered for this research. One is from Sri Lanka and the other routing table is from USA. Simulation results presented on Table 2 proves current BGP best route selection is not fully efficient. A 50 per cent of best routes are decided based on local router ID or lowest interface IP which does not have any significance to Internet routing. This can cause high latency to a particular destination. In addtion router administrators cannot change this routing decision since changing interface IPs and routers ID are not possible after setting up network. BGP communities can help to resolve this issue up to some extent, but it depends on upstream ISP capabilities. Most ISPs does not properly implement BGP communities.

A positive relationship between latency and end user experience was identified especially for web page browsing. Therefore ISPs need to reduce inter AS latency as much as possible in order to achieve better end user experience. As described above, BGP is the only protocol used by ISPs to route traffic among Autonomous Systems. Therefore, this research proposal suggests introducing new route selection criteria to BGP route selection algorithm. This research expect this criteria need to adopt protocol itself rather than control route section based on optional BGP policy configurations.

3.1 Proposed New Addition to BGP Route Selection Algorithm

This proposal suggest to consider geo location of IP address in addition to AS PATH attribute of standard BGP protocol to decide BGP best route in case of existing algorithm finds matching AS_PATH for a particular destination. Below is the proposed best path selection algorithm

Table 2 : Proposed Modification to BGP route Selection Algorithm

1. Discarding the routes with the unreachable Next_Hop.
2. Preferring the route with the highest Local_Pref.
3. Preferring the aggregated route. The preference of an aggregated route is higher than the preference of a non-aggregated route.
4. Preferring the route with the shortest AS-Path.

5. If AS-Path finds equal, consider shortest GEO distance. If still distance is same follow next steps.
6. Comparing the Origin attribute and selecting the routes with the Origin attribute as IGP, EGP, or Incomplete in order.
7. Preferring the route with the smallest MED value.
8. Preferring the route learned from EBGP. The preference of an EBGP route is higher than that of an IBPG route.
9. Preferring the route with the smallest IGP metric in an AS. Load balancing is performed according to the number of configured routes if load balancing is configured and there are multiple external routes with the same AS-Path.
10. Preferring the route with the shortest Cluster List.
11. Preferring the route with the smallest Originator ID.
12. Preferring the route advertised by the router with the smallest router ID.
13. Comparing IP addresses of the peers and preferring the route that is learnt from the peer with a smaller IP address.

This research proposes to include item 5 in to current BGP route selection algorithm. Below section explains how to calculate GEO distance to particular destination.

3.2 Geo Region Classification.

This proposal suggests use standard country code as geo graphic region ID for particular IP block. Current country code list is attached in Appendix 1. If further granularity is required, it is possible to aim for the country-city code.However, this proposal considers only county code for route selection algorithm.

3.2.1 Assumptions

There are two basic assumptions in this proposal.

1. Particular ISP does not have more than one upstream ISP connectivity to a particular country. If two more links exit, routing algorithm consider steps 6 to 13 for best route selection.
2. When peering or transit, ISP selects the shortest distance POP. For example if India wants to select POP at Singapore, two paths are available due to round nature of the world; path one is through the east segment of world and path two is through the west segment of the world. India selects path through East by default. In other case short distance path need to be selected.

3.2.2 IP to Country Mapping.

According to current practice any IP block must register in regional IP registry before it announces through BGP protocol. This process is called creating "route" object in regional IP registry. All major ISPs verify regional routing registry database periodically before any IP block advertise to upstream. Figure 22 demonstrates current settings of "route" object. It is suggested adding two new mandatory fields called "usg-rgn" denoting usage region and geo filed denoting geo graphic location. This could be similar to country code filed in current "route" object specification but it is not mandatory to equal country code and usg-rgn. Large ISPs register IP blocks under original country but they spans all over the world. For example, tier 1 ISP from USA can register all IPs belonging to them under country code 1. Nevertheless, ISP can operate throughout the world. In this case, country field of route object can be USA and usg-rgn need to update according to actual usage country. For example, usg-rgn for IP blocks advertise from Netherland POP is 31. Usg-rgn for IP blocks advertise from Singapore POP is 65. Geo filed is actual longitude and latitude of POP, which routes are, advertised.

Any BGP speakers expect to synchronize regional IP database periodically to extract latest updates. This proposal suggests receiving updates weekly basis.

```
                Status        Instance      Search Status

route:          [mandatory]   [single]      [primary/lookup
 key]
descr:          [mandatory]   [multiple]    [ ]
country:        [optional]    [single]      [ ]
origin:         [mandatory]   [single]      [primary/invers
e key]
holes:          [optional]    [multiple]    [ ]
member-of:      [optional]    [multiple]    [inverse key]
inject:         [optional]    [multiple]    [ ]
aggr-mtd:       [optional]    [single]      [ ]
aggr-bndry:     [optional]    [single]      [ ]
export-comps:   [optional]    [single]      [ ]
components:     [optional]    [single]      [ ]
remarks:        [optional]    [multiple]    [ ]
notify:         [optional]    [multiple]    [inverse key]
mnt-lower:      [optional]    [multiple]    [inverse key]
mnt-routes:     [optional]    [multiple]    [inverse key]
mnt-by:         [mandatory]   [multiple]    [inverse key]
changed:        [mandatory]   [multiple]    [ ]
source:         [mandatory]   [single]      [ ]
```

Figure 22: Definition of route Object

Source: https://www.apnic.net/apnic-info/whois_search/using-whois/guide/route

3.3 Calculations

Each router expects to calculate outgoing interface for each IP block on an offline basis. Repetition of this calculation based on sync period of routing database with regional IP registry. In this proposal, it is one week.

In this calculation, it is assumed ISP has n number of upstream ISPs.

Table 3: Notations

Upstream ISP	I_i i=1,2,3,4,….n
Longitude of upstream ISP POP	Lon_{Ii}
Latitude of upstream ISP POP	Lat_{Ii}
Interface index	1,2,3,4,…….n
Longitude of usg-rgn in Country code K	Lon C_K K=1,2,3,……..1000
Latitude of usg-rgn in Country code K	Lat C_K K=1,2,3,……..1000
Longitude of POP i in Country code K	Lon Ci_K K=1,2,3,……..1000,i=1,2,3…n
Latitude of POP i in Country code K	Lat Ci_K K=1,2,3,……..1000,i=1,2,3….n

Shortest Distance from i^{th} upstream ISP to Country K	D_{iK}
Shorted distance to country K	D_K

Assume there is n number of POPs setup at country X. Hence we can find n number of usg-rgn geo locations from regional routing database for a particular country code. Therefore, we need to get average coordinates for those n numbers of POPs. We may achieve this by adding all longitudes of POPs and then divide by n. Similarly, by adding all latitudes of POPs and divide by n. This will generalize one virtual POP location for a country.

$$\text{Lon } C_K = \frac{\sum_{i=0}^{n} \text{Lon CiK}}{n}$$

$$\text{Lat } C_K = \frac{\sum_{i=0}^{n} \text{Lat CiK}}{n}$$

$$D_{iK} = \min\{(\text{Lon } I_{i,} \text{ }_{\text{Lat}} I_i) - \text{POP}(\text{Lon } C_{K,}\text{Lat } C_K)\} \quad i=1,2,3\ldots.n$$

$$D_K = \min (D_{iK})$$

Above calculation, fills table 4. It is referred to link index.

Table 4: Country Code vs Best Outgoing Interface

Country code	Best upstream link index
1	3
2	8
3	1
n	n

3.4 Calculating flow table

We have already calculated best outgoing interfaces for each country code considering geo graphic distance from local router. This proposal suggests considering /24 IP blocks since it is the minimum length allowed advertising in ISP environment. It is assumed that single route has maximum 256 upstream connections. Table 5 refers required memory to store GOE routing table in memory. In this proposal, it is suggested to keep GEO routing table completely in memory to achieve software lookup efficiently.

Table 5: Memory Requirement to Keep GEO routing Table

Number of /24 IP blocks in current IPV4 address space	14614528
Reserved /24 IP blocks (Appendix 2)	218117
Total usable IP blocks	14396411
Bytes required to store /24 IP block	4
Bytes required to store outgoing interface	1
Total byte required to store Geo routing table/ (MB)	70

Sample GEO routing table is presented in Table 6.

Table 6: Sample GEO Routing Table

Route	Outgoing index
16777216 (1.0.0.0/24)	1
16777472 (1.0.1.0/24)	6
16777728 (1.0.2.0/24)	8
| | | |	
3758096128 (223.255.255.0/24	255

Chapter 4

RESULTS

4.1 Relationship between Latency and Web Page Loading Time

This research has two objectives. Objective one is to identify whether any relationship exists latency and end user experience. End user experience is measured in terms of web page loading time.

According to W3C Working Draft 13 January 2016, web page lading pass several steps. In this research, following criteria was considered as web page loading time.

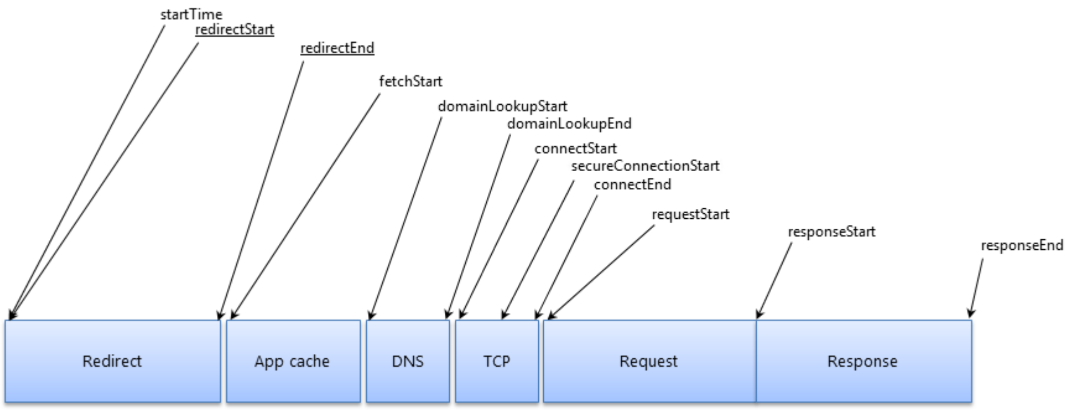

Figure 23: Timing Components of Web Page Loading

Web page loading Time = responseEnd – StartTime

Following setup was used to measure web page loading time with different delay introduced to incoming and outgoing packets.

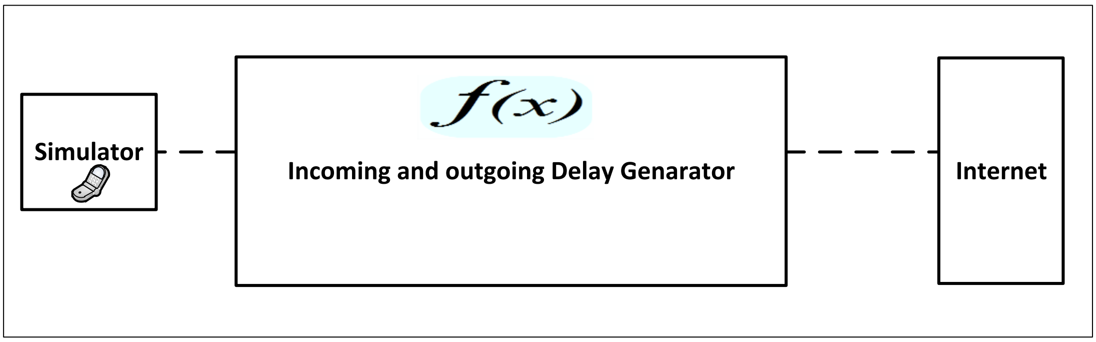

Figure 24: Simulation Setup for Web Page Loading Time.

The research considered following popular URLs in Sri Lanka for measuring latency vs. web page loading time.

- http://www.google.lk
- http://www.facebook.com
- http://yahoo.com
- http://www.cnn.com
- http://www.bbc.com
- http://ikman.lk
- http://www.hirunews.lk
- http://bing.com
- http://www.divaina.com

4.1.1 Test Result for www.google.lk

Table 7: Page Load time vs. latency for www.google.lk

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.google.lk	1.60	2.25	5.87	8.12	10.53

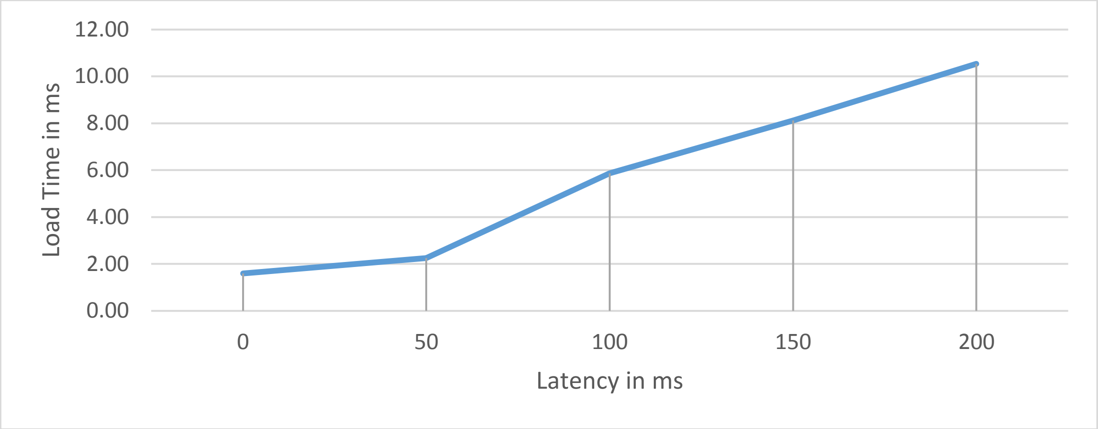

Figure 25: Latency vs. Page load Time for www.google.lk

4.1.2 Test Statistics for www.facebook.com

Table 8: Page Load time vs. latency www.facebook.com

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.facebook.com	2.11	2.84	6.02	7.94	9.99

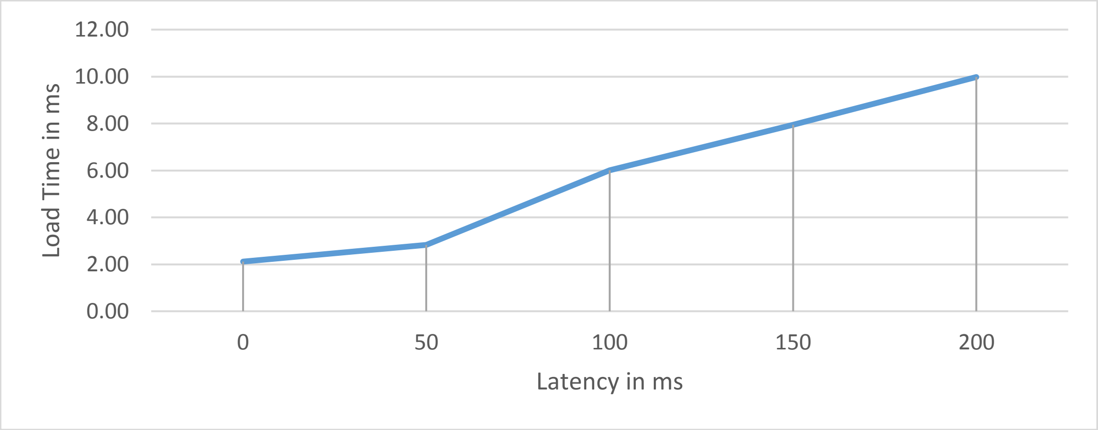

Figure 26: Latency vs. Page load Time for www.facebook.com

4.1.3 Test Statistics for www.cnn.com

Table 9: Page Load time vs. latency for www.cnn.com

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.cnn.com	7.25	28.47	30.50	32.45	40.52

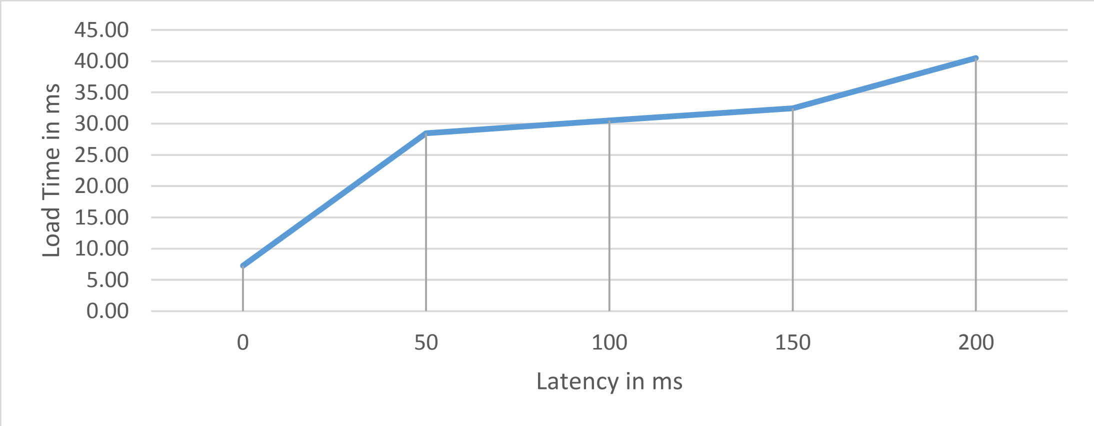

Figure 27: Latency vs. Page load Time for www.faacebook.com

4.1.4 Test Statistics for www.bbc.com

Table 10: Page Load time vs. latency for www.bbc.com

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.bbc.com	3.88	7.53	17.17	22.76	27.74

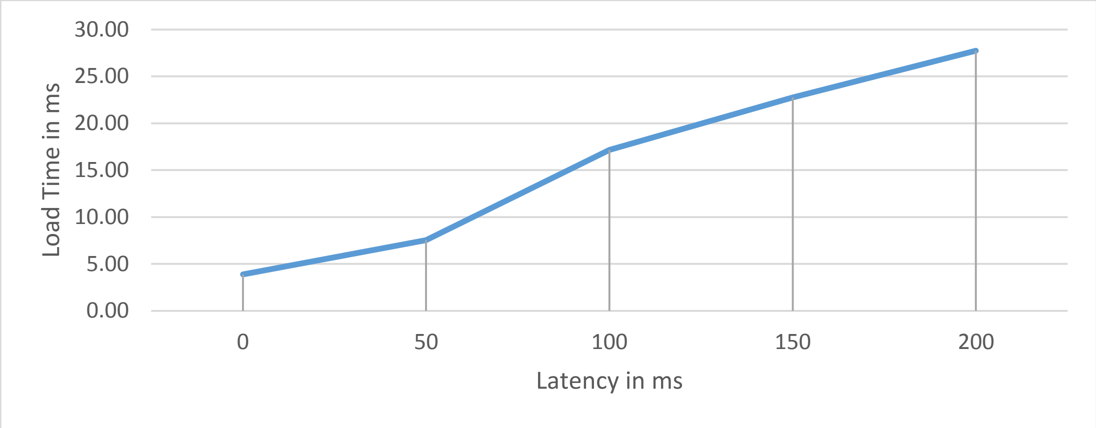

Figure 28: Latency vs. Page load Time for www.bbc.com

4.1.5 *Test Statistics for ikman.lk*

Table 11: Page Load time vs. latency for www.ikman.lk

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.ikman.lk	1.44	2.80	7.35	10.12	13.14

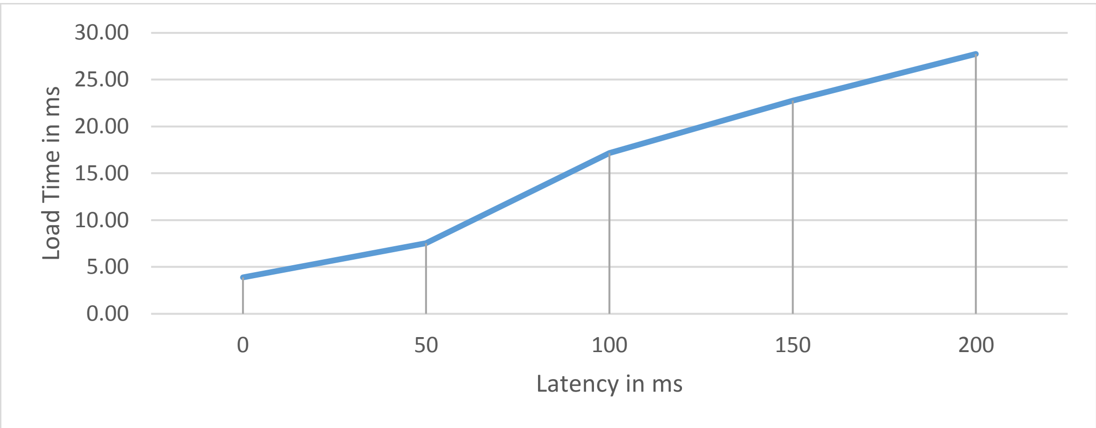

Figure 29: Latency vs. Page load Time for www.ikman.lk

4.1.6 *Test Statistics for www.hirunews.lk*

Table 12: Page Load time vs. latency for www.hirunews.lk

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.hirunews.lk	10.34	12.87	43.83	31.80	29.27

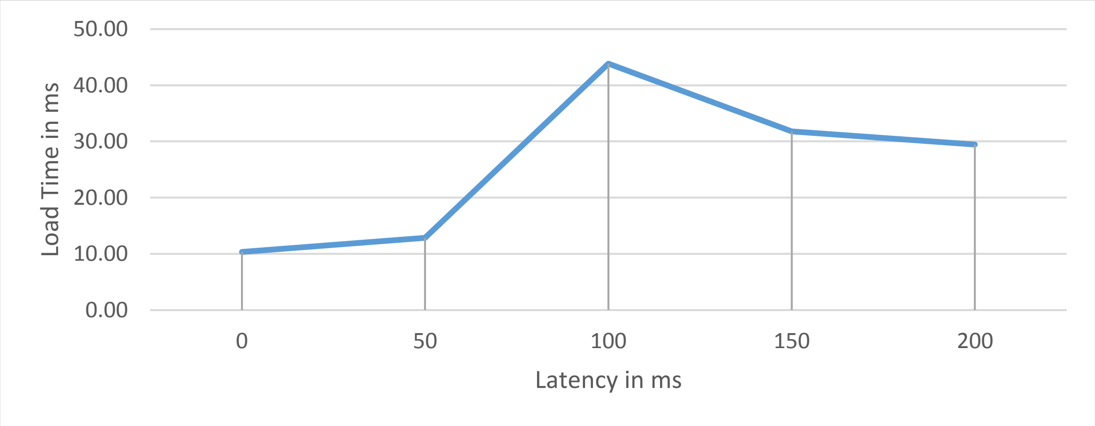

Figure 30: Latency vs. Page load Time for www.hirunews.lk

4.1.7 *Test Statistics for www.bing.com*

Table 13: Page Load time vs. latency for www.bing.com

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.bing.com	0.58	1.14	2.96	3.89	4.99

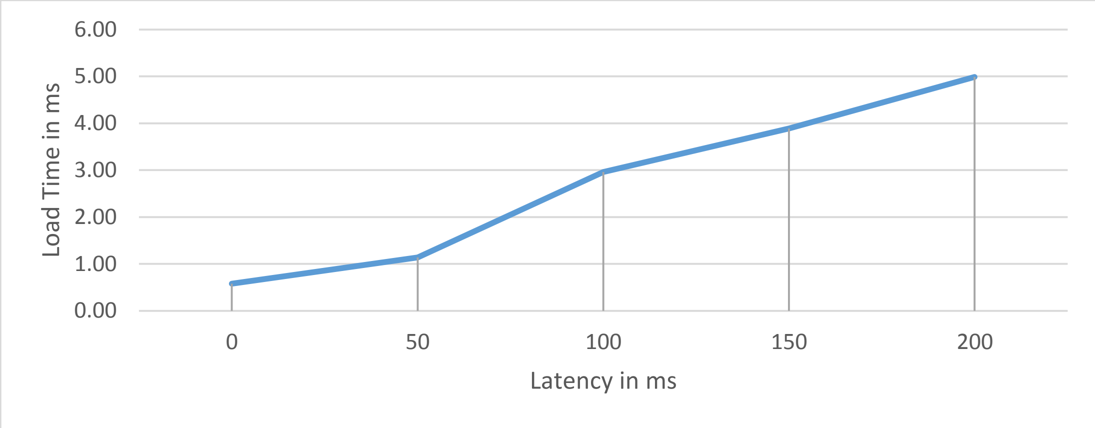

Figure 31: Latency vs. Page load Time for www.bing.com

4.1.8 Test Statistics for www.divaina.com

Table 14: Page Load time vs. latency for www.divaina.com

Web Page	Simulated Radio and Access Network Delay in ms				
Delay	0	50	100	150	200
www.divaina.com	2.35	2.57	3.48	8.72	11.68

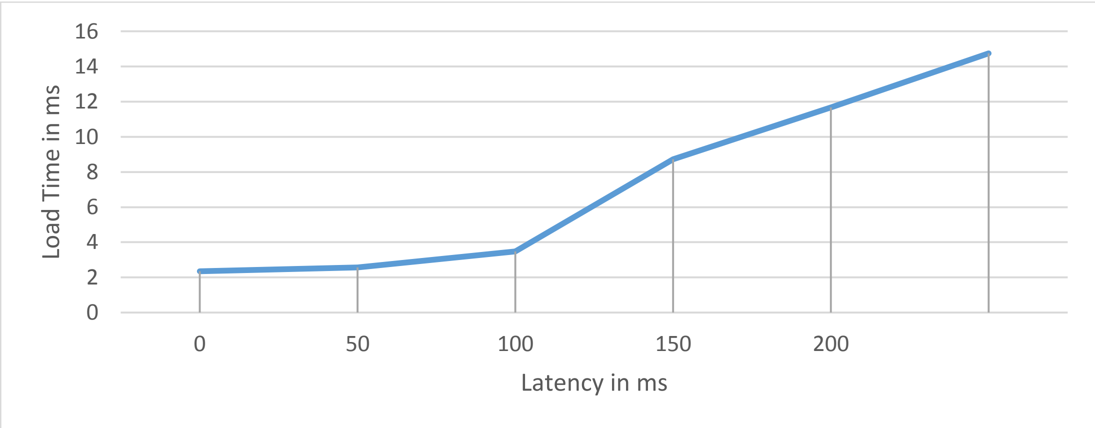

Figure 32: Latency vs. Page load Time for www.divaina.com

Based on above test statistics, a positive relationship between latency and web page loading time is evident. Therefore, service providers need to optimize latency to any destination as much as possible.

4.2 BGP Routing Table Analysis for Equal AS_PATH

Service providers can initiate several actions to reduce network latency. In this research, I have focused only on ISP network latency optimization. Service provider core network and access network optimization are other possibilities.

ISPs use BGP protocol to exchange route between Autonomous numbers. BGP best path selection influences to latency to particular destination. This research introduces new criteria to BGP best path selection algorithm using GEO location of route origination. Simulation is performed with a java program to get an idea of on how many routes have match to equal AS path in current 5 million BGP routing table. GEO calculation is planned to implement with QUAGGA Routing Suite for a reference. GEO routing table calculation is suggested to conduct in an offline mode once a week. Therefore, there is no impact to routing selection with proposed GEO routing calculation. Simulation proved that a valid opportunity to introduce GEO routing in case of equal AS-PATH in multi-homing environment.

Table 15: Simulation Result

ISP Location	Number of Routes	AS-PATH Match	%
Sri Lanka	541,199	350,377	64
USA	200,000	102,000	51

Above simulation result shows more than 50% route selection occurs randomly may be according to BGP router ID. This will not guarantee best outgoing path selected by BGP route selection algorithm. Hence, requirement of new route selection criteria arises for tie breaking scenario. Proposed geo routing is the suggested solution for this issue.

Chapter 5

SDN BASED IMPLEMENTATION

5.1 SDN Architecture

Networking technologies have evolved slower compared to other communication technologies. Network equipment such as switches and routers were traditionally developed by individual manufacturers with their own firmware and other software to operate their own hardware in a proprietary and closed way. This slowed the progress of innovations in networking technologies and caused an increase in management and operation costs whenever new services, technologies or hardware was to be deployed within existing networks. The architecture of today's networks consist of three core logical planes: Control plane, data plane, and management plane. A software-defined networking (SDN) architecture defines how a networking and computing system can be built using a combination of open, software-based technologies and commodity networking hardware that separate the control plane and the data layer of the networking stack.

Traditionally, both the control and data plane elements of a networking architecture were packaged in proprietary, integrated code distributed by one or a combination of proprietary vendors. The OpenFlow standard, created in 2008, was recognized as the first SDN architecture that defined how the control and data plane elements would be separated and communicated with each other using the OpenFlow protocol. Figure 33 shows conceptual architecture of SDN.

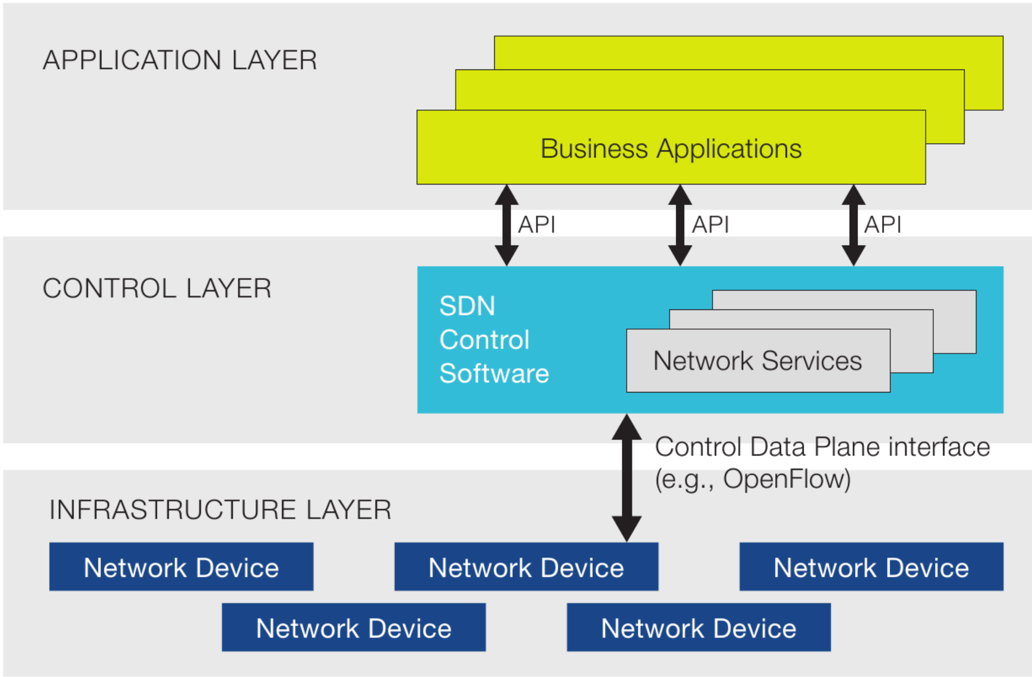

Figure 33: SDN Architecture

Source: https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture

So far, networks hardware has been developed with tightly coupled control and data planes. Thus, traditional networks are known to be "inside the box" paradigm [11]. This significantly increases the complexity and cost of network administration and management. Being aware of these limitations, networking research communities and industrial market leaders have collaborated to rethink the design of traditional networks. Thus, proposals for a new networking paradigm, namely programmable networks [11], have emerged. The principal endeavors of SDN are to separate the control plane from the data plane and to centralize network's intelligence and state. Therefore, it is easy to influence routing decision in routers using SDN architecture. I am discussing SDN architecture because proposed GEO routing can be easily implemented in controller of SDN router.

5.1.1 *Proposed SDN Implementation*

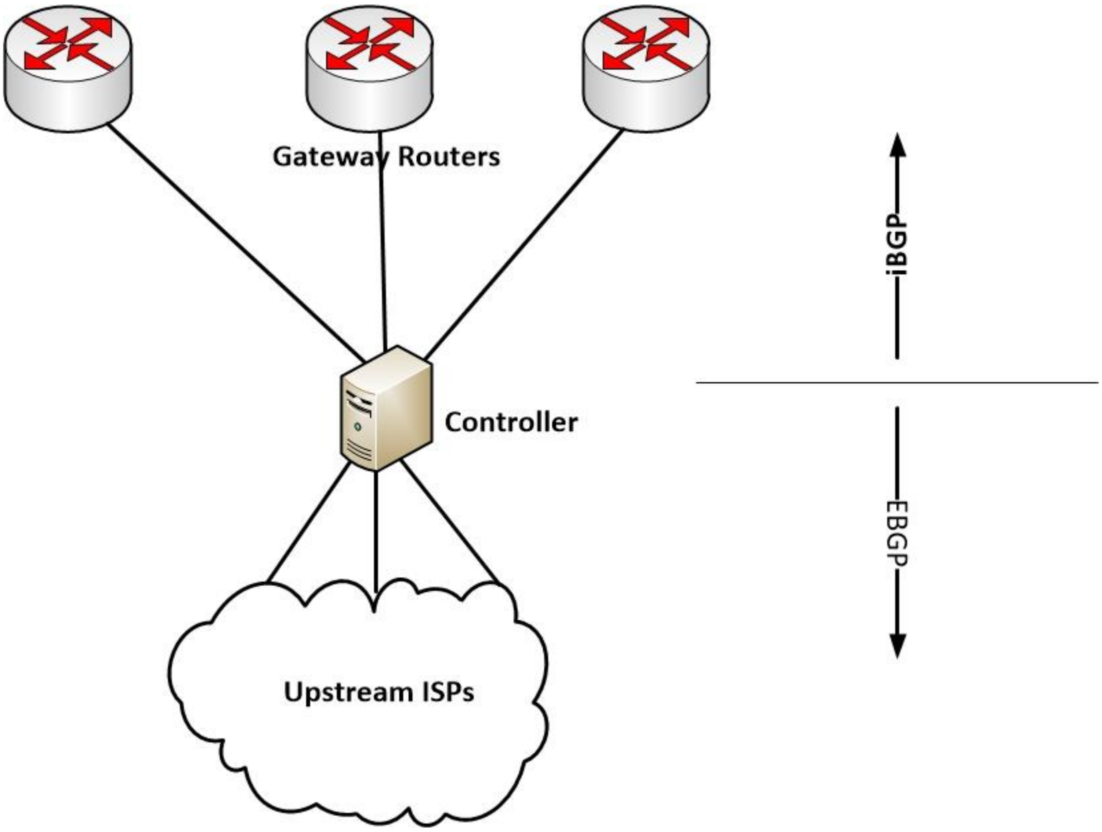

Figure 34: Proposed SDN based implementation

BGP- 4 was originally introduced in 1994 and now has become a stable and widely adopted protocol. There is no major change to the core of protocol since 1994 except two byte to four-byte accommodation. There are several updates since 1994 but all these changes are proposed as optional configurations. Therefore, it is very difficult to implement proposed GEO based routing architecture with legacy BGP implementation. However, according to SDN architecture, control plane separates from data plane. Thus new route filtering logic can be implemented easily with SDN architecture. Figure 34 presents network setup which can be implemented through SDN based architecture. In this setup controller setups EBGP relationship with upstream ISPs. Similarly, controller setups IBGP with gateway routers. IBGP session distribute next-hop IP address according to proposed Geo based routing algorithm.

Chapter 6

CONCLUSION AND FUTURE WORK

Aim of this research is to propose new route selection criteria to BGP best path selection algorithm. BGP is the only routing protocol currently used in ISP environment. Rekhter and T. Li. Introduced in 1994 in RFC 1654. As described in this the research proposal, protocol is well defined and widely used globally. There are several suggestions to BGP protocol since 1994, however the original implementation is not much changed. This could be due to large adaptation of BGP protocol throughout in the world. Most modifications on BGP protocol in ISP environment are based on optional parameters. When we analyze current BGP route selection methods in addition to original proposal, all route selections are based on BGP community based implementations. However, BGP community is an optional parameter in BGP standard and a unique standard for BGP communities is lacking. Some large ISPs add BGP community string indicating route origination location when advertising to his customers and peers. End routers need to apply complex route policies to select the best outgoing path. This requires good technical and programming knowledge to route administrators. Route policy implementation can vary from vendor to vendor and upstream ISP to ISP.

Accuracy of location marking depends on the upstream ISP capabilities. If BGP protocol does not select the proper path to destination in ISP environment, end users experience high latency to destination. Further unnecessary traffic flows occur in different part of the world. For example, if USA are to send traffic to Japan, incorrect BGP path selection can select traffic via Europe-Asia instead direct USA Japan routes. By considering all these factors, this proposal suggests new criteria for BGP route selection algorithm, when existing route section algorithm detects equal AS path to destinations.

When we study existing BGP implementation, the difficulty in changing existing BGP route selection algorithm in legacy hardware is easily identified .This is due to several vendor implementations of BGP protocol and thousands of routes deployed all over the world. No guarantee ensures that all routers are updated with new implementation, even vendors implement proposed modifications. However, SDN is still new to the world and under research to deploy SDN based routers all around the worlds. Thus, still there is a space to introduce new algorithm to SDN based routers. Therefore I suggest implementing the proposed GEO based route selection criteria in SDN based routers. However, there is no objection to implement the same algorithm in legacy hardware.

BGP is a heavily adopted protocol in the internet domain. It is hard to change such a stable implementation to achieve proposed geo based routing. However, the current world trend is towards SDN architecture. Therefore SDN based implementation has a clear future for this proposal. Further, more success of this proposal depends on number of deployments. If all routers check geo distance before outgoing path is selected, expected output can achieved. Since SDN implementations are ongoing with all vendors, it is good to start thinking on embedding geo based routing protocol itself rather than options feature.

This proposal suggests calculating geo distance based on the coordinates. Considering actual cable distance instead of coordinate based distance calculation, can be improve the outcome. Therefore, incorporating cable distance is a future possibility, which is proposed in this research.

Incorporating geo distance and link congestion state to route selection process need to be mandatory with SDN based routing implementation and is another key highlight proposed in this research.

REFERENCES

[1] Wikipedia, "http://en.wikipedia.org/wiki/Internet.," [Online]. Available: Wikipedia. http://en.wikipedia.org/wiki/Internet.. [Accessed 10 10 2015].

[2] L. T. Rekhter Y, *A Border Gateway Protocol 4 (BGP-4).Request For Comments 1771,* Internet Engineering Task Force, 1995.

[3] mobileapps, "http://mobileapps.gov.kn/?q=node/14," [Online]. Available: http://mobileapps.gov.kn/?q=node/14. [Accessed 10 10 2015].

[4] http://www.itcertnotes.com, "http://www.itcertnotes.com/2012/01/bgp-message-types.html," [Online]. Available: http://www.itcertnotes.com/2012/01/bgp-message-types.html. [Accessed 10 10 2015].

[5] R. J. Caesar M, "BGP Routing Policies in ISP Networks," *Network, IEEE,* vol. 19, no. 6, pp. 5-11, 2005.

[6] H. G. M. E. Andrew T. C, "A Survey of Programmable Networks," *SIGCOMM Comput. Communication,* vol. 29, no. 2, pp. 7-23, 1999.

[7] J. ,. R. R. Alzate, "Evaluation of improvement proposals for Border Gateway Protocol (BGP)," *Communications Conference (COLCOM),* pp. 1-6, 2012.

[8] "Optimal Configuration for BGP Route Selection," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies,* vol. 2, pp. 916-926, 2003.

[9] "Inbound Traffic Load Balancing in BGP Multi-homed Stub Networks," *Distributed Computing Systems, 2008. ICDCS '08. The 28th International Conference,* pp. 369-376, 2008.

[10] B. J. Nieto-Hipolito J.I, "On the Geographical Properties of BGP," *High Performance Switching and Routing,* pp. 221-226, 2003.

[11] M. T. M. Jarraya Y, "A Survey and a Layered Taxonomy of Software-Defined Networking," *Communications Surveys & Tutorials,* vol. 16, no. 4, pp. 1955-1980, 2014.

APPENDIX -1

Table 16: List of Country Codes

COUNTRY	COUNTRY CODE	ISO CODES
Afghanistan	93	AF / AFG
Albania	355	AL / ALB
Algeria	213	DZ / DZA
American Samoa	1-684	AS / ASM
Andorra	376	AD / AND
Angola	244	AO / AGO
Anguilla	1-264	AI / AIA
Antarctica	672	AQ / ATA
Antigua and Barbuda	1-268	AG / ATG
Argentina	54	AR / ARG
Armenia	374	AM / ARM
Aruba	297	AW / ABW
Australia	61	AU / AUS
Austria	43	AT / AUT
Azerbaijan	994	AZ / AZE
Bahamas	1-242	BS / BHS
Bahrain	973	BH / BHR
Bangladesh	880	BD / BGD
Barbados	1-246	BB / BRB
Belarus	375	BY / BLR
Belgium	32	BE / BEL
Belize	501	BZ / BLZ
Benin	229	BJ / BEN
Bermuda	1-441	BM / BMU
Bhutan	975	BT / BTN
Bolivia	591	BO / BOL

Bosnia and Herzegovina	387	BA / BIH
Botswana	267	BW / BWA
Brazil	55	BR / BRA
British Indian Ocean Territory	246	IO / IOT
British Virgin Islands	1-284	VG / VGB
Brunei	673	BN / BRN
Bulgaria	359	BG / BGR
Burkina Faso	226	BF / BFA
Burundi	257	BI / BDI
Cambodia	855	KH / KHM
Cameroon	237	CM / CMR
Canada	1	CA / CAN
Cape Verde	238	CV / CPV
Cayman Islands	1-345	KY / CYM
Central African Republic	236	CF / CAF
Chad	235	TD / TCD
Chile	56	CL / CHL
China	86	CN / CHN
Christmas Island	61	CX / CXR
Cocos Islands	61	CC / CCK
Colombia	57	CO / COL
Comoros	269	KM / COM
Cook Islands	682	CK / COK
Costa Rica	506	CR / CRI
Croatia	385	HR / HRV
Cuba	53	CU / CUB
Curacao	599	CW / CUW
Cyprus	357	CY / CYP
Czech Republic	420	CZ / CZE
Democratic Republic of the Congo	243	CD / COD
Denmark	45	DK / DNK

Djibouti	253	DJ / DJI
Dominica	1-767	DM / DMA
Dominican Republic	1-809	DO / DOM
East Timor	670	TL / TLS
Ecuador	593	EC / ECU
Egypt	20	EG / EGY
El Salvador	503	SV / SLV
Equatorial Guinea	240	GQ / GNQ
Eritrea	291	ER / ERI
Estonia	372	EE / EST
Ethiopia	251	ET / ETH
Falkland Islands	500	FK / FLK
Faroe Islands	298	FO / FRO
Fiji	679	FJ / FJI
Finland	358	FI / FIN
France	33	FR / FRA
French Polynesia	689	PF / PYF
Gabon	241	GA / GAB
Gambia	220	GM / GMB
Georgia	995	GE / GEO
Germany	49	DE / DEU
Ghana	233	GH / GHA
Gibraltar	350	GI / GIB
Greece	30	GR / GRC
Greenland	299	GL / GRL
Grenada	1-473	GD / GRD
Guam	1-671	GU / GUM
Guatemala	502	GT / GTM
Guernsey	44-1481	GG / GGY
Guinea	224	GN / GIN
Guinea-Bissau	245	GW / GNB

Guyana	592	GY / GUY
Haiti	509	HT / HTI
Honduras	504	HN / HND
Hong Kong	852	HK / HKG
Hungary	36	HU / HUN
Iceland	354	IS / ISL
India	91	IN / IND
Indonesia	62	ID / IDN
Iran	98	IR / IRN
Iraq	964	IQ / IRQ
Ireland	353	IE / IRL
Isle of Man	44-1624	IM / IMN
Israel	972	IL / ISR
Italy	39	IT / ITA
Ivory Coast	225	CI / CIV
Jamaica	1-876	JM / JAM
Japan	81	JP / JPN
Jersey	44-1534	JE / JEY
Jordan	962	JO / JOR
Kazakhstan	7	KZ / KAZ
Kenya	254	KE / KEN
Kiribati	686	KI / KIR
Kosovo	383	XK / XKX
Kuwait	965	KW / KWT
Kyrgyzstan	996	KG / KGZ
Laos	856	LA / LAO
Latvia	371	LV / LVA
Lebanon	961	LB / LBN
Lesotho	266	LS / LSO
Liberia	231	LR / LBR
Libya	218	LY / LBY

Liechtenstein	423	LI / LIE
Lithuania	370	LT / LTU
Luxembourg	352	LU / LUX
Macao	853	MO / MAC
Macedonia	389	MK / MKD
Madagascar	261	MG / MDG
Malawi	265	MW / MWI
Malaysia	60	MY / MYS
Maldives	960	MV / MDV
Mali	223	ML / MLI
Malta	356	MT / MLT
Marshall Islands	692	MH / MHL
Mauritania	222	MR / MRT
Mauritius	230	MU / MUS
Mayotte	262	YT / MYT
Mexico	52	MX / MEX
Micronesia	691	FM / FSM
Moldova	373	MD / MDA
Monaco	377	MC / MCO
Mongolia	976	MN / MNG
Montenegro	382	ME / MNE
Montserrat	1-664	MS / MSR
Morocco	212	MA / MAR
Mozambique	258	MZ / MOZ
Myanmar	95	MM / MMR
Namibia	264	NA / NAM
Nauru	674	NR / NRU
Nepal	977	NP / NPL
Netherlands	31	NL / NLD
Netherlands Antilles	599	AN / ANT
New Caledonia	687	NC / NCL

New Zealand	64	NZ / NZL
Nicaragua	505	NI / NIC
Niger	227	NE / NER
Nigeria	234	NG / NGA
Niue	683	NU / NIU
North Korea	850	KP / PRK
Northern Mariana Islands	1	MP / MNP
Norway	47	NO / NOR
Oman	968	OM / OMN
Pakistan	92	PK / PAK
Palau	680	PW / PLW
Palestine	970	PS / PSE
Panama	507	PA / PAN
Papua New Guinea	675	PG / PNG
Paraguay	595	PY / PRY
Peru	51	PE / PER
Philippines	63	PH / PHL
Pitcairn	64	PN / PCN
Poland	48	PL / POL
Portugal	351	PT / PRT
Puerto Rico	1	PR / PRI
Qatar	974	QA / QAT
Republic of the Congo	242	CG / COG
Reunion	262	RE / REU
Romania	40	RO / ROU
Russia	7	RU / RUS
Rwanda	250	RW / RWA
Saint Barthelemy	590	BL / BLM
Saint Helena	290	SH / SHN
Saint Kitts and Nevis	1	KN / KNA
Saint Lucia	1	LC / LCA

Saint Martin	590	MF / MAF
Saint Pierre and Miquelon	508	PM / SPM
Saint Vincent and the Grenadines	1	VC / VCT
Samoa	685	WS / WSM
San Marino	378	SM / SMR
Sao Tome and Principe	239	ST / STP
Saudi Arabia	966	SA / SAU
Senegal	221	SN / SEN
Serbia	381	RS / SRB
Seychelles	248	SC / SYC
Sierra Leone	232	SL / SLE
Singapore	65	SG / SGP
Sint Maarten	1	SX / SXM
Slovakia	421	SK / SVK
Slovenia	386	SI / SVN
Solomon Islands	677	SB / SLB
Somalia	252	SO / SOM
South Africa	27	ZA / ZAF
South Korea	82	KR / KOR
South Sudan	211	SS / SSD
Spain	34	ES / ESP
Sri Lanka	94	LK / LKA
Sudan	249	SD / SDN
Suriname	597	SR / SUR
Svalbard and Jan Mayen	47	SJ / SJM
Swaziland	268	SZ / SWZ
Sweden	46	SE / SWE
Switzerland	41	CH / CHE
Syria	963	SY / SYR
Taiwan	886	TW / TWN
Tajikistan	992	TJ / TJK

Tanzania	255	TZ / TZA
Thailand	66	TH / THA
Togo	228	TG / TGO
Tokelau	690	TK / TKL
Tonga	676	TO / TON
Trinidad and Tobago	1	TT / TTO
Tunisia	216	TN / TUN
Turkey	90	TR / TUR
Turkmenistan	993	TM / TKM
Turks and Caicos Islands	1	TC / TCA
Tuvalu	688	TV / TUV
U.S. Virgin Islands	1	VI / VIR
Uganda	256	UG / UGA
Ukraine	380	UA / UKR
United Arab Emirates	971	AE / ARE
Uzbekistan	998	UZ / UZB
Vanuatu	678	VU / VUT
Vatican	379	VA / VAT
Venezuela	58	VE / VEN
Vietnam	84	VN / VNM
Wallis and Futuna	681	WF / WLF
Western Sahara	212	EH / ESH
Yemen	967	YE / YEM
Zambia	260	ZM / ZMB
Zimbabwe	263	ZW / ZWE

Source: https://countrycode.org/

APPENDIX-2

Table 17: Reserved IP blocks

Address block (CIDR)	Number of Addresses	Scope	Purpose
0.0.0.0/8	16,777,216	software	Used for broadcast messages to the current ("this") network as specified by RFC 1700, page 4.
10.0.0.0/8	16,777,216	private network	Used for local communications within a private network as specified by RFC 1918.
100.64.0.0/10	4,194,304	private network	Used for communications between a service provider and its subscribers when using a Carrier-grade NAT, as specified by RFC 6598.
127.0.0.0/8	16,777,216	host	Used for loopback addresses to the local host, as specified by RFC 990.
169.254.0.0/16	65,536	subnet	Used for link-local addresses between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server, as specified by RFC 3927.
172.16.0.0/12	1,048,576	private network	Used for local communications within a private network as specified by RFC 1918
192.0.0.0/24	256	private network	Used for the IANA IPv4 Special Purpose Address Registry as specified by RFC 5736
192.0.2.0/24	256	documentation	Assigned as "TEST-NET" in RFC 5737 for use solely in documentation and example source code and should not be used publicly.

192.88.99.0/24	256	Internet	Used by 6to4 anycast relays as specified by RFC 3068.
192.168.0.0/16	65,536	private network	Used for local communications within a private network as specified by RFC 1918.
198.18.0.0/15	131,072	private network	Used for testing of inter-network communications between two separate subnets as specified in RFC 2544.
198.51.100.0/24	256	documentation	Assigned as "TEST-NET-2" in RFC 5737 for use solely in documentation and example source codeand should not be used publicly.
203.0.113.0/24	256	documentation	Assigned as "TEST-NET-3" in RFC 5737 for use solely in documentation and example source codeand should not be used publicly.
224.0.0.0/4	268,435,456	Internet	Reserved for multicast assignments as specified in RFC 5771.
			233.252.0.0/24 is assigned as "MCAST-TEST-NET" for use solely in documentation and example source code.
240.0.0.0/4	268,435,455	n/a	Reserved for future use, as specified by RFC 6890.
255.255.255.255/32	1	n/a	Reserved for the "limited broadcast" destination address, as specified by RFC 6890.

Source: https://en.wikipedia.org/wiki/Reserved_IP_addresses