www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.18088-18095

Compatibility of Border Meeting of Two Layers Protocol (BGP Version 4) With IPV6

Yashpal Yadav[1], Madan singh [2], Vikas Kumar[3]

1Assistant Prof., Dept. Computer Science & Engineering, SRM University, Ghaziabad, UP, India

2, Assistant Prof., Dept. Computer Science & Application, SRM University, Ghaziabad, UP, India

3, Assistant Prof., Dept. Computer Science & Application, SRM University, Ghaziabad, UP, India

Abstract

This paper deals with issues, which network designers, would have to deal with once IPV6, which is the layer 3 Internet Protocol of the future comes into mass existence. IPV6 will have compatibility issues with most of the existing routing protocols especially with Border Gateway Protocol (BGPV4), which is a layer 7 protocol on which the backbone of the Internet runs. BGP Version 4 is an interdomain routing protocol. The primary function of BGP is to provide and exchange network reachability information between Autonomous Systems (AS).

In this paper, we have dealt with only one problem out of the many, which we believe will arise, once both BGPV4 and IPV6 co-exist. We, in our crest to explore the issues of compatibility between the two different protocols, have observed that a lot of research has gone into IPV6, but none whatsoever is been followed up on modifying BGPV4 in accordance to IPV6. The reason for this could probably be that since IPV6, is still at a nascent stage of implementation in real world, the grave problems are yet to be dealt with as far as routing protocols are concerned. We believe since IPV6's implementation is inevitable, the issues raised in this paper will have to be dealt with at some point in the future and the solution proposed is a step in that direction.

Keywords: BGP, IPV6, Multicast backbone (MBONE),

Introduction

In the early 1980s, the routers that made up the APRANET ran a distance vector protocol known as the Gateway-to-Gateway protocol (GGP). Every router knew the route to every reachable network. But as the size of APRANET grew their routing protocol did not scale well. So APRANET moved from one big network to interconnection of many networks which came to be known as AS (Autonomous System). An administrative authority manages its AS and chooses the routing protocol on its routers (IGP). Today RIP, Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF) and Integrated System to Intermediate System (IS-IS) have replaced GGP. Each AS is connected to other AS through one or more exterior gateways. These exterior gateways share routing information using Exterior Gateway Protocol (EGP). Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP). BGP is an application layer protocol. BGP Version4 is the most recent version of BGP, which supports CIDR (classless interdomain routing). But with the introduction of IPV6, we believe this would have to change. BGP V4 is not fully compatible with IPV6. Our paper throws light at these issues and proposes modifications to BGP V4 algorithm

BACKGROUND

BGP V4 is defined in RFC 1771 (March 1995). The primary function of BGP is to provide and exchange network reachability information between AS's. BGP is usually configured between

two directly connected routers that belong to two different AS. Each AS is under different technical administrator. Before routing updates can be exchanged between two BGP routers must become established neighbors i.e. establish a TCP session between each other. After BGP routers

establish a TCP connection, they become established neighbors and start exchanging routing information. The exchange of information takes place in form of data packets encapsulated in the segments.

The routing information exchanged is:

1) BGP Version number
2) AS number
3) BGP router ID

The border gateway protocol (BGP), defined in RFC1771, provides loop free interdomain routing between autonomous system.(An autonomous system is set of router that operates under the same administration .) BGP is often run among the networks of Internet service providers (ISPs). This case study examines how BGP works and how you can see it to participate in routing with other networks that run BGP. Before it exchanges information with an external AS, BGP ensures that networks within the AS are reachable. This is done by a combination of internal BGP peering among routers within the AS and by redistributing BGP routing information to Interior Gateway Protocols (IGPs) that run within the AS, such as Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF).

BGP can establish two types of peering relationships:

- **IBGP**
- **EBGP**

IBGP describes the peering between two BGP neighbors in the same AS. With IBGP the external routes learned are shared between the BGP routers on the same AS since IGP running on interior routers does not understand AS Path and BGP attributes. EBGP describes BGP peering between neighbors in different AS (Autonomous regions).

Enhanced Interior Gateway Routing Protocol: - Abbreviated as EIGRP, an evolved version of IGRP that addresses the demands of large-scale Internet works and the changes in network technology that has been developed since the implementation of IGRP. Routers that already use IGRP can use EIGRP because the metrics for both protocols are directly translatable, i.e., they are as easily comparable as if they were routes that originated in their own autonomous systems.

Interior Gateway Routing Protocol: - Abbreviated as IGRP, a proprietary network protocol, developed by Cisco Systems, designed to work on autonomous systems. IGRP is a distance-vector routing protocol, which means that each router sends all or a portion of its routing table in a routing message update at regular intervals to each of its neighboring routers. A router chooses the best path between a source and a destination. Since each path can comprise many links,

the system needs a way to compare the links in order to find the best path. A system such as RIP uses only one criteria -- hops -- to determine the best path. IGRP uses five criteria to determine the best path: the link's speed, delay, packet size, loading and reliability. Network administrators can set the weighting factors for each of these metrics. **CIDR**: - Classless Inter-Domain routing, an IP addressing scheme that replaces the older system based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP network prefix. For example: 172.200.0.0/16.CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations. CIDR is also called supernetting.

BORDER GATEWAY PROTOCOL: The border gateway protocol (BGP), defined in RFC1771, provides loop free interdomain routing between autonomous system. (An autonomous system is set of router that operates under the same administration.) BGP is often run among the networks of Internet service providers (ISPs). This case study examines how BGP works and how you can see it to participate in routing with other networks that run BGP.

BGP Fundamentals

This section presents fundamentals information about BGP, Including the following topics:

- Internal BGP
- External BGP
- BGP and routes maps

- Advertising Networks

Attributes of BGPV4

BGP is a simple protocol that uses attributes to make a selection of best path to a destination. BGP attributes can be categorized as well known or optional. Well-known attributes are recognized by all BGP implementations. Optional attributes do not need to be supported by BGP process. BGP selects only one path as the best path. When the path is selected, BGP puts the selected path in its routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:

If the path specifies a next hop that is inaccessible, drop the update. Prefer the path with the largest weight. If the weights are the same, prefer the path with the largest local preference. If the local preferences are the same, prefer the path that was Attributes are divided into two broad categories. **A Well-known and optional. A well-known** attribute is one that every BGP router should recognize. **An optional** attribute is one that need not be recognized by every router. Well-known attribute are they divided into two categories:

1. **Mandatory**
2. **Discretionary.**

A well-known mandatory attribute is one that must appear in the description of route. A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message. One well-known mandatory attribute is ORIGIN. This defines the source of routing information (RIP and OSPF).

BACKBONE: -At the border of an area, special router called area border router summarizes the information about the area and sends to other area. Among the areas inside an autonomous system is a special area called the backbone; All the area inside an autonomous system mu8st be connected to the backbone. The backbone serves as a primary area, and other area serve as the secondary area. The router inside the backbone is called the backbone routers.

Multicast backbone (MBONE):-A multicast router may not found another multicast router in the neighborhood to forward the multicast packet. Although this problem may be solved in the next few years by adding more and more multicast routers, there is another solution for this problem. The solution is **Tunneling**. To enable multicasting, we make a multicast backbone out of these isolated router, using the concept of tunneling. The multicast router may not be connected physically, but they are connected logically.

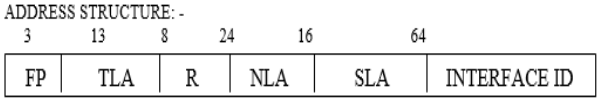
IPV6 (internet protocol version 6): -

Version 4 of the Internet protocol places an upper limit on how the Internet can grow. It employs 32-bit addressing scheme. Network designers have been utilizing 'Network Address Translation' (NAT) to extend the life of IPV4 and CIDR (classless interdomain routing) to use the address space efficiently. In future every house will need an IP address and Internet cell phone, IP watch, a networked car will be a reality. Only way to realize this is implementing Internet protocol on IPV6. In 1995, the Internet task force (IETF), which develops protocols standard for the internet, issued a specification for next generation IP known then as IPng. IPv6 provides number of functional enhancement over the exiting IP.The current Ip uses a 32-bit address to specify a source or destination. IPV6 includes 128-bit source and destination address field.IPV6 addresses are represented in hexadecimal divided into eight 16-bit pieces.

This form is represented as:

X: X: X: X: X: X: X: X

ADDRESS STRUCTURE: -



Challenges

Border meeting of two Layers: -

The industry is fast thinking of moving to IPV6, but that thought is limited to various authorities of Internet who are having a tough time now finding an alternate solution to the depleting IP addresses of version 4. The ISP's who don't plan to expand there reachability or the companies who have no plan of expanding any further as far as there network is concerned are very reluctant to covert to IPV6 scheme as the

DOI: 10.18535/ijecs/v5i9.49

extra cost could prove to be phenomenal. So now what we have is a border meeting of the two layer 3 protocols, namely IPV4 AND IPV6. So the question now is whether the BGP can manage to differentiate between both the schemes and actually in this way break away with layer schemes that has been in existence ever since networking concept arose. It is a very big issue and needs to be addressed in great details because the backbone networks of NAP would be probably will soon want to adapt the IPV6 scheme. End users of NAP i.e. ISP's or may be some Company which possess a valid AS identity would be reluctant to switch over to IPV6.If the above situation arises, definitely the BGP session peering would have a problem as the Open Message Format would have differences in the version number of the BGP. This could be explained better with the help of a diagram and layered analysis of the way BGP peers with the other, AS's border router as on today and complexity, which will arise when IPV6 support version of BGP is implemented.

Capabilities Negotiation with BGP 4: -BGP Capabilities Negotiation provides a mechanism to introduce new features to BGP like in this case if BGP needs to support IPng it would negotiate for the previous supported version of the BGP which would be the version 4, which is actually a backward compatibility factor added to every new version of BGP. The difference this time would be that the change is taking place at Layer-3 and to support that change, modifications are to done in the BGP layer 7 protocols. Change at two layers simultaneously is what the whole problem-causing factor is, which would be touched upon later.

BGP Neighbor Negotiation one of the basic steps of the BGP protocol is establishing sessions between BGP peers. Without successful completion of this step, the exchange of updates will not occur. Neighbor negotiation is based on the successful completion of a TCP transport connection, the successful processing of the OPEN message, and periodic detection of the UPDATE or KEEPALIVE messages.

Open Message Format:-

The figure below shows the OPEN message which BGP peers share when to establish connection.

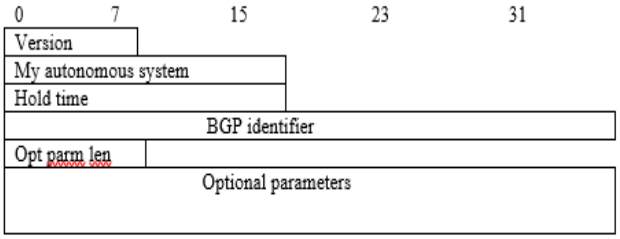


Fig. Open Message Format

OPEN message:-In the above shown header format we would now like to focus just on the version field and its implications as in today's Internet layer-7 protocol BGP.In fig. the field name, version is discussed below:

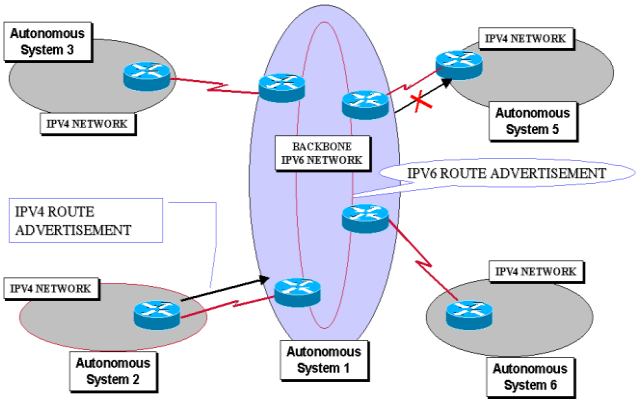
1. A 1-byte unsigned integer that indicates the version of the BGP message, such as BGP-3 or BGP-4. During the neighbor negotiation, BGP peers agree on a BGP Version number. BGP peers negotiate the lowest common version that they both support.

They reset the BGP session and renegotiate until a common supported version is determined by the peers. Now this is what would prove to be a problem-causing factor. This could be explained better with the help of a real time scenario which would actually exist when BGP new version is introduced along with the introduction of IPV6 which in initial phase would only be applied at the main backbone of the internet at various geographical locations and slowly and steadily spread out to the end users. Let us consider the situation when the process of IPv6 is only introduced at the backbone and the end users (in this case the ISP's) would still be sticking on with the IPv4 and BGPv4.

2. An open message to create a neighborhood relationship, a router running BGP opens a connection with a neighbor and sends an open message. if the neighbor accepts the neighborhood relationship, it responds with a keep-alive message, which means that a relationship has been established between the two routers.

DOI: 10.18535/ijecs/v5i9.49

3. But the major question that arises up is how will the routers communicate and transaction with each other i.e. different AS. How the boundary routers are connected to each other's through a BACKBONE. The backbone stores all the reachability information about various boundary routers. Now when a reachability information of one AS needs to be sent to another AS via the backbone, developing of the peer relationship would cause a problem between the backbone routers and the peer AS routers. The two border router would negotiate for a lower version of BGP i.e.BGPv4 that would not support the IPv6.So the payload would not carry the IPv6 reachability information to the peer AS through the reachability information would reach the backbone router. So the situation would be that the backbone routers would be acting as stub AS.



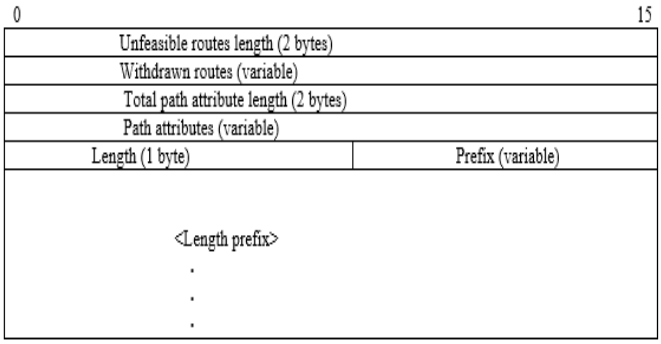
Interconnection of Two AS using Bone

The entire boundary router is connected to others with BONE. BONE is also worked as a area boundary router. This has stored all the reachability information but cannot transfer to other autonomous system. So how you can solve these types of problems. How can data transfer to different level? With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP network prefix. BGP Version4 is the most recent version of BGP, which supports CIDR (classless interdomain routing). But with the introduction of IPv6, we believe this would have to change. BGP V4 is not fully compatible with IPv6. Our paper throws light at these issues and proposes modifications to BGP v4 algorithm. The backbone has all the reachability information of all the peers but is not able to pass on the information any further. This could be thought of as a situation that is acceptable if the number of networks were low in which you provide static routing to the backbone routers and since backbone has the information about the reachability to the other AS's it would pass on the traffic. But what if every day new addresses are being learnt by the backbone with more and more people joining in to the backbone. It would be required to keep making addition of static routing, which is not an intelligent solution.

Then one could even think of providing default gateway to each AS for the traffic leaving the system. But the problem with this kind of solution is that traffic which is not reachable via backbone, a request for it would still be made by the peer AS and traffic would be finally dropped at the backbone. A clear-cut case of waste of bandwidth.

Solution to the Problem: -

The Problem is basically with header format and needs to be changed. Consider the header once again of the Update.



Change IP Header Format

Central to the BGP protocol is the concept of routing updates. Routing updates contain all the necessary information that BGP uses to construct a loop-free picture of the network. The following are the basic blocks of an UPDATE message:

- **Network Layer Reachability Information (NLRI)**
- **Path Attributes**

• Unfeasible Routes

The NLRI field, of update message supports IPv4 payload. The proposed solution is that the version negotiation should be stopped by the equipment's on which these protocols are running like done on Cisco router. This solution provides that when no negotiations for the version take place, backbone should manage to carry the IPv6 payload within its updates i.e. 128 bits NLRI. The header support to IPv6 payload. Hence the problem of BGP updating the peers with IPV6 reachability is solved but another problem Aries related with understanding of IPv6 payload by peer AS i.e. situation where a peer is running on IPv4 has routing table entries of IPv6. So the question is whether the layer 3 protocol be forward compatible. Consider the situation once again with respect to layer 3 & not layer 7. Here reachability updates coming from an AS to the backbone are in IPv4 format, which is therefore converted into the IPV6 format according to the interoperability of IPv6.Therefore routing information stored in border route table in Ipv6 format IPV6 information is provided at the peer, which from layer 7 gets directly placed at the route table in form of Ipv6. But the layer 3 does not support Ipv6 so the entry would actually make no difference w.r.t. IPv4. However, the solution to this is already under testing, where the feature is to design the IPv6 in such a manner that if a IPv4 is converted to IPv6 format and forwarded to another IPv4 running router, then it would be able to read the IPv4 original address.

So now we would have solved the problem of BGP updating the peers with IPV6 reachability. However, the solution to this is already under testing, where the feature is to design the IPv6 in such a manner that if a IPv4 is converted to IPv6 format and forwarded to another IPv4 running router, then it would be able to read the IPv4 original address.

CONCLUSION

Function BGP was designed to allow routers (called gateways in the standard) in different autonomous systems (Ass) to cooperate in the exchange of routing information. The protocol use message, which are sent over TCP connection .The repertoire of message .The current version of BGP is known as BGP-4 (RFC-1771)

The functional procedures are involved in BGP:

- Neighbor acquisition
- Neighbor reachability
- Network reachability

Two routers are considering being neighbors if they are attached to the same sub network. If the two router are in different autonomous systems they may wish to exchange routing information. For this purpose, it is necessary to first perform **neighbor acquisition.** To perform neighbor acquisition, two router send Open message to each other after a TCP connection is established. If each router accepts the request, it returns a Keep-alive message in response. Once a neighbor relationship is established, the **neighbor reachability** procedure is used to maintain the relationship. Each partner needs to be assured that the other partner still exists and is still engaged in the neighbor relationship. The final procedure specified by BGP is **network reachability**. Each router maintains a database of the sub networks that it can reach and preferred route for reaching that network. When a change is made to this database, the router issues an Update message that is broadcast to all other routers that implement BGP.

REFERENCES

[1] RFC 1519 (CIDR Design)

[2] RFC 1771, "Border Gateway Protocol 4"

[3] RFC 1997, "BGP Communities Attributes"

[4] RFC 793, "Transmission Control Protocol"

[5] RFC 2460, "Internet Protocol, Version 6 Specifications." S. Hinden, S.Deering, Dec 1998

[6] RFC 2373, "Internet Protocol, Version 6 Addressing Architecture." S. Hinden, S.Deering, Dec 1998

[7] Computer Networks By Andrew S. Tanebaum towards Processing System.

[8] Computer Network and Internet By Douglas E. Comer.

[9] Computer Networking With Internet Protocol and Technology By, " WILLIAM STALLING".

[10] BLAC00 Black, U.IP Routing Protocols: RIP, OSPF, BGP, PNNI & Cisco Routing Protocols.

[11] HIND 95 : R."IP Next generation Overview." Connexion, March1995.

[12] THOM96: Thomas, S.IPng and the TCP/IP Protocols: Implementing the Next Generation [13] Internet. New York:Wiley,1996

[14] Internet routing architecture by Sam Hallabi

[15] Routing TCP/IP Volume II by Jeff Doyle

[16] TCP/IP routing Design and Management by Karl Solie