Aftab et al LGURJCSIT 2019

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 3, July - September 2019

ANALYSIS OF BORDER GATEWAY PROTOCOL, ITS TYPES AND MEASURES TO AVOID RISK

Aftab Ahmad Malik[1], Anas Riaz[2], Haroon Ur Rashid Kayani[3], Waqar Azeem[4]
Department of Software Engineering[1,2,3] Department of Computer Science[4]
Lahore Garrison University, Lahore
dr_aftab_malik@yahoo.com

Abstract:

This is the age of digital communication. The process involves sending messages from one end of the network to other end using the internet, extranets and the Internet of Things (IOT) Technologies. Initially, the internet is a small community. But today internet becomes a global community as thousands of different administrative entities own and operate the internet. The process of transferring data across the network is known as routing. The process of routing is performed by using routers. Routers use certain protocols to achieve this task. The Broader Gateway Protocol (BGP) is an interdomain routing protocol that is used to connect two different autonomous systems. The autonomous system is collection of network that runs under a single administrative entity. This paper includes analysis and important techniques of border gateway protocol, types of BGP, its attributes, security threats and measures to avoid risks.

Keywords: AS, BGP, IBGP, EBGP.

1. Introduction

We are living in the world of digital communication. The digital communication involves the mechanism of sending message from one end to other ends of the network. The process of transferring the message across the internet is a complex task. The process of sending packets from one end to another on the network is known as routing. The mechanism of routing involves special networking devices known as routers [1]. The router is an intelligent device that connects different networks. The connection can be either using wired or wireless. In the OSI model, the router operates at the network layer. Routers have their own memory, processing unit, and input-output interfaces. Routers have routing tables that store the information about the path from source to destination. Incoming and outgoing messages are filtered by these devices based on the sender and receiver addresses [2]. A message from source is forwarded to routers which then forward these packets to the destination using information. The main source of communication between routers is routing protocols. Using these protocols, information about the destination is changed between routers and path is selected [1]. The routing protocol can be defined as the set of rules designed for routers that will specify the best path between the source and destination [2] and also specifies how different routers will communicate with each other.

The process of routing is classified as:

a. Static Routing
b. Dynamic Routing

We know that the routers have knowledge about each device on the network. The information is received from either the neighbor router or from the administrator of the network [3]. In other words, routers are configured either manually by the network administrator or they will generate routing table automatically without Static routing is a mechanism in which routers are configured manually by the network administrator [4]. Static routes once configured cannot be changed with a change in the network

unless the administrator changes it. But static routing is not fault-tolerant. In case of any failure, the traffic will not be re-routed. On the other hand, dynamic routing does not involve manual configuration of routing tables. Instead dynamic routing use protocols to maintain routing tables. Network changes are adopted automatically[4].

Table 1: Dynamic Routing Protocols

Sr. No.	Dynamic Protocol
1.	RIP (Routing Information Protocol)
2.	IGRP (Interior Gateway Routing Protocol)
3.	EIGRP (Exterior Gateway Routing Protocol)
4.	OSPF (Open Shortest Path First)
5.	IS-IS (Intermediate System- Intermediate System)
6.	BGP (Border Gateway Protocol)

The table above enlists some common types of dynamic routing protocols. The main focus of this paper is the Border gateway protocol and its types.

1. Evolution of Border Gateway Protocol:

Initially, the internet was just like a tiny cloud, at that time the small number of networks was connected to each other. The routing between these nodes is done using a static routing approach. The task to be done at that time was just to identify, configure and connect different nodes of the network which can be done easily using static routing. But now the internet is considered as a collection of many different networks that run under a single administration. More and more networks are interlinked. With the growth of the internet, it requires some dynamic routing protocols. At that time, Exterior Gateway Protocol (EGP) was invented[5]. On the internet, each network running under the single administration is referred to as an autonomous system. EGP is a routing protocol that will distribute information between different autonomous systems. The protocol deals with how communication between different autonomous systems will occur [6]. With the increase in the number of Autonomous Systems (ASS), the drawbacks of EGP become prominent. EGP has a tree-like structure initially, but afterward, the tree topology was replaced by mesh topology. The hierarchical structure makes the connections of new devices difficult and scalability was also affected [5]. Also, EGP does not support multipath networking environment. To overcome these flaws a new routing protocol was invented. This new protocol was named as Border Gateway Protocol.

2. Border Gateway Protocol:

BGP is the most popular and commonly used inter-domain routing protocol. It is the protocol that makes the internet work [7]. When routing takes place within a single autonomous system, it is referred to as interdomain routing. Certain policies are designed for inter-domain routing [8]. It is an exterior gateway protocol. BGP was introduced to communicate between different Autonomous Systems (ASs) [9]. An AS is a network that operates under the administration of a single administrator. BGP is a distance vector routing protocol. It is also referred to as the path-vector routing protocol. Distance vector routing that uses distance and decides the best path to transfer packet. Using a consistent transportation mechanism, routing updates are forward to all BGP neighbors. TCP is used for reliable transportation of packets. BGP uses port 179 of TCP/IP [8].

As discussed earlier, the BGP protocol is used to communicate between different AS's. A routing table is maintained that keeps a record of all routes to reach the destination. The information gets updated dynamically with the change in layout of the network. Once a complete routing table is exchanged among all neighbors upon any change; only that change will be updated [10]. The neighbors of BGP are known as their peers. Contrary to other IGP protocols, BGP does not have the ability to search its neighbor. There is manual configuration of neighbors. The router that is configured to run BGP protocol is named as BGP speaker. Within the same or different as the BGP speakers connect to each other using TCP port and share the routing information. Peering can be internal within the same autonomous system or external between different autonomous systems. While the connection is alive the BGP peers communicate by sharing messages [11].

When BGP session is established first an open message is sent between BGP peers. The message contains information about the version

of BGP, the number of local AS, and router ID. It is compulsory that the version of BGP on both peers is same. After every 60 seconds of session establishment, a keep-alive message is exchanged between the peers. The message will ensure that the peer is available and accessible. The hold time period for the peer is 180 seconds and if the router does not receive the keep-alive message after hold time, the peer is considered to be dead. To exchange the routes between different peers BGP transfer update messages. When any error occurs during communication, a notification message is delivered and the session broke down [9].
Common message header used by all BGP peers is divided into 4 parts. The part along with byte length is shown in figure below:

Marker	Length	Type	Data
16	2	1	variable

Figure 1 : BGP Message Header

When data is delivered to the application layer the format of the data in the payload is unknown. Only the port number and IP address are identified by TCP port. Data is recognized as a stream of data and BGP uses the marker field to mark the start byte of each message. The type field is used to identify the type of message being sent. Type will represent whether the message is update message, keep-alive or other types of messages[12].

During the formation of session, BGP passes through several states. This is known as Finite State Machine (FSM). The states of FSM are described below:

a. Idle State:

In the idle state, the BGP ignores requests; it will start TCP connection with its BGP peers. It will also listen to connections from their peers. After that, the state changes from idle to connect[9].

b. Connect State:

On the successful establishment of session, BGP will not spend much time in this state. BGP will wait for peer negotiation. It will send an open message to its peer and change its state from connecting to open sent state [9].

c. Active State:

If the router will not establish TCP session, it will terminate in active state. After that FSM will retry to establish a TCP session. If the session is established an open message is delivered to the peer. If the session is not established the FSM will move back to the idle state. On repeated failures, a cycle is established between the active and idle state[9].

d. Open Sent State:

BGP will receive open messages from their peers. After receiving messages validity of the open message is checked by the router. If an error occurs at this state a notification message along with the error detail is retransmitted to the peer and if the message does not contain any error a keep-alive message with several timers are transmitted to the peer. The state is set to Open confirm [9].

e. Open Confirm State:

The peer will receive keep-alive messages. If the messages are not expired BGP will move to establish the state. If the timer expires before the keep-alive message is received or any other error is found the router will move back to idle state[9].

f. Established State:

In this state, information is exchanged between peers by sending update messages. In case of errors, the notification message is delivered and the router is set back to idle state[9].

3. PATH ATTRIBUTES:

The routing information in BGP is generated by using path-vector algorithm. Routing Information Base (RIB) is maintained to store the data or path attributes. Path attributes are categorized as:

a. Well-known Mandatory:

These attributes must be implemented on all

BGP peers. They must be the part of every update message and must be updated on top priority. Origin, AS path, destination and next are some of the important well known mandatory attributes[13].

b. Well-known Discretionary:

These are the attributes that are not a compulsory part of updated message. But these attributes are recognized by all BGP peers. Like LOCAL_PREF [13].

c. Optional Transitive:

Transitive attributes are those which are checked by the peers; if any attribute is not recognized by them. Intransitive attribute transitive flag is checked. If the flag is turned set the peers will accept the attribute. Also, the attribute will be advertised to all peers [13].

d. Optional non-Transitive:

These are the attributes that if not identified the message can be ignored and not advertised to peers [13].

3.2. Types of BGP:

There are two types of BGP. These are as follows:

a. IBGP
b. EBGP

When BGP session is established between peers within a single autonomous system; the session is established using IBGP or interior border gateway protocol. When the session is established between peers belonging to two different autonomous systems the protocol used is EBGP or exterior border gateway protocol.
The figure below shows the IBGP network.

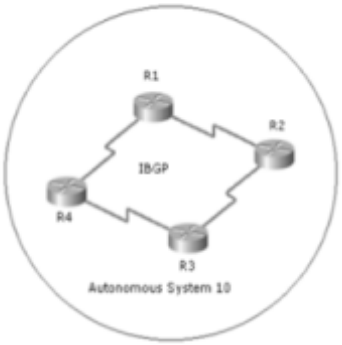

Figure 2 : IBGP network

There are several routing protocols that are used to route the information within AS. These protocols involve OSPF, RIP, EIGRP and many more. In IBGP all peers are connected in a full mesh topology.

While in EBGP communication between two different autonomous systems takes place. BGP is configured at the edge router of the AS. While the communication between two edge routers takes place using EBGP [14].

4. Route Reflectors and Confederations:

Mesh topology introduces some scalability issues. For example, if we have a total of N routers in our autonomous system, there will be (N-1) IBGP peers and (N*(N-1)) BGP sessions. If we take a small ISP network that contains 100 routers with BGP running in them, It would create 99 IBGP neighbors and 4950 BGP sessions in total.

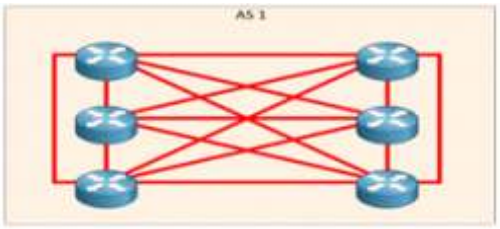

Figure 3 : Mesh Topology

In the above figure, we have an autonomous system; in AS we have 6 routers that are connected in a full mesh. Each router is connected directly to other routers. The topology gives advantage in that routers have multiple paths to communicate with each other if one path goes down the router can use an alternate path to communicate. Messages are transferred between IBGP peers directly. But this topology will result in a lack of stability. When BGP sessions increase in number the processing will put the load on processing. The burden can be much more than a router can handle. If we want to add a new device it means that we have to configure all devices in the network which would be a complex task [15].

Route reflectors and route confederations were introduced to get rid of mesh topology. To prevent looping and to improve management and scalability; we use the technique of route reflector; in this case, the above diagram will become as:

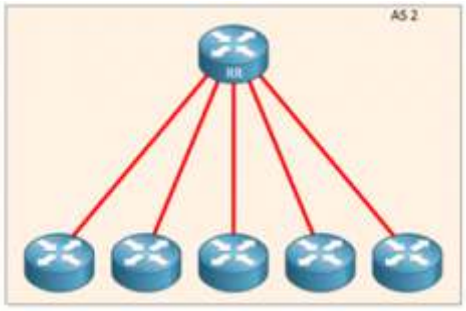

Figure 4 : Router Reflectors

We still have 6 routers. Each router is connected directly to route reflector. When any router will advertise any route to reflector it is reflected to all routers through route reflector. Using this technique scalability is improved and configuration is simplified. The main drawback of this technique is that what if the reflector goes down.

In the BGP confederation, the AS subdivision takes place. The subdivision will decrease the number of BGP peering.

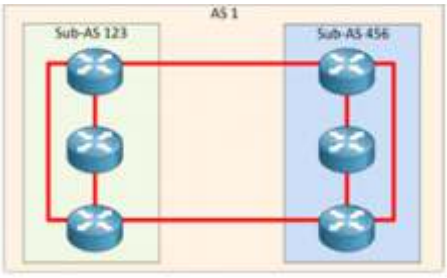

Figure 5 : BGP Confederations

It can be seen that by using BGP confederation the number of BGP peering reduces from 15 to 8. But inside the AS the topology used is mesh topology [15].

4. BGP Attacks:

Routers are exposed to denial of service, unauthorized access, eavesdropping, session hijacking and other types of attacks. Denial of service occurs when the number of packets is more than a router can handle. Some of the denials of service attacks are listed below.

Table 2: Types of BGP Attacks

Sr. no.	Attack Type	Explanation
1	Starvation	Nodes do not receive all packets as the packets may be delivered to inactive nodes due to excessive traffic.
2	Black-hole	Some or all of the packets are dropped by the router.
3	Delay	Sub optimal paths are used for delivery of packets.
4	Looping	Traffic is never delivered because packets enter in looping path.
5	Network Partition	Due to fault in routing information the network is divided. Part of network is divided from rest of the network.
6	Churn	Packet delivery is disrupted due to changes in packet forwarding.

Unauthorized access is possible when the password is guessed or it is not changed. Social engineering or misuse of software flaws also results in unauthorized access. Because BGP messages are not encrypted the eavesdropping of BGP packets may take place on path anywhere between routers. Using the incorrect IP addresses or inserting wrong data in routing tables may become the reason for packet manipulation. Session hijacking involves the use of false packets to continue an authorized session by some unauthorized source [10].

4.2. Protection and Security:

Securing BGP mainly involves protecting the router on which BGP is running. The first step to protect the router is to keep and operate the router in a secure room. Only the administrator or authorized persons are allowed to visit the room. Provide constant power supply to the routers so to reduce the chances of a router failure.

5. Conclusion:

This paper includes an analysis of border gateway protocol. As the internet is a collection of different autonomous systems. There is a need to connect these different AS, so BGP was mainly designed for this purpose. It is an Exterior gateway protocol that connects two different AS. When the BGP session is between routers of the same AS, the used is an interior gateway protocol and when connection is between different AS's the protocol used is exterior gateway protocol. The main issue in mesh topology is the scalability which is reduced by the BGP route reflectors and confederations. In this paper, the security risks and their solutions is also discussed.

6. Acknowledgement

The authors acknowledge the encouragement of Shazia Saqib the chief editor and the Dean Faculty of Computer Science, Lahore Garrison University.

References:

[1]. IANA. (2016). Border Gateway Protocol (BGP) Parameters. Retrieved from http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml

[2]: https://www.lifewire.com/how-routers-work-816456

[3]: http://www.firewall.cx/networking-topics/routing/routing-protocols.html

[4]. Deng, J., Wu, S., & Sun, K. (2014). Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET, 23. Retrieved from http://www.sfu.ca/~sihengw/ENSC427_Group9/Final Report .pdf

[5]: https://www.google.com.pk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwiuh7msxHYAhXva5oKHRoDCSUQFghgMAc&url=https%3A%2F%2Fwww.incapsula.com%2Fblog%2Fbgp-routing-explained.html&usg=AOvVaw3O fkiN-YcNEroJy_dSa2_F4

[6]: http://www.thenetworkencyclopedia.com/entry/ exterior-gateway-protocol-egp/

[7]. Xuehui, W. (2013). BGP Fast Convergence Based on Message Classification, 6(6), 151–160.

[8]. Bhagat, N. H. (2012). Border Gateway Protocol – A Best Performance Protocol when used for External Routing than Internal Routing. International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA, 3(2), 29–32.

[9]: Protocol, B. G., Version, B. G. P., Vector, P., Path, A. S., Systems, A., & Systems, B. G. P. A. (2007). - Border Gateway Protocol -, 1–30.

[10]: Caesar, M., & Rexford, J. (2005). BGP routing policies in ISP networks. IEEE Network, 19(6), 5–11. https://doi.org/10.1109/MNET.2005.1541715

[11]: http://www.brocade.com/content/html/en/configuration-guide/nos-601-

l3guide/GUID-0E73E334-69D8-4FDE-8CEC-B1F0F98D6B9D.html

[12]: https://ahmedmuhi.wordpress.com/2012/09/03/marker-field-in-bgp-message-header/

[13]: Kuhn, R. (2007),"Border Gateway Protocol Security Recommendations of the National Institute of Standards and Technology", (July).

[14]: Bhagat, N. H. (2012). Border Gateway Protocol – A Best Performance Protocol when used for External Routing than Internal Routing. International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA, 3(2), 29–32.

[15]: http://lostintransit.se/2013/09/09/ibgp-fully-meshed-vs-route-reflection/