ISSN 2348 – 9928
IJAICT Volume 3, Issue 12, December 2016 Doi:01.0401/ijaict.2014.07.15 Published on 05 (12) 2016

AN SURVEY ON INTERDOMAIN ROUTING USING BORDER GATEWAY PROTOCOL

Ms. V. Sharmila
PG Scholar,
Information Technology,
SNS College of Technology,
Coimbatore, Tamilnadu, India

Mr. M. Kalimuthu
Associate Professor,
Information Technology,
SNS College of Technology,
Coimbatore, Tamilnadu, India

Abstract— This paper presents the loop free inter domain routing using BGP which means that it enables the communication between two autonomous system using Border Gateway Protocol without any loop. In this, BGP is proposed by enabling the OSPF protocol within the autonomous system, where OSPF is a dynamic protocol that dynamically updates the routing information that helps to forward the packet from source and destination. The Border Gateway Protocol (BGP) is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used 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 for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. This paper includes introduction, advantages and its limitations, basic BGP configuration, BGP attributes, working of BGP and protocol overview.

Keywords— Autonomous System, Loop, Inter domain Routing, Protocol, Routing, Attributes.

I. INTRODUCTION

The Internet is a global, decentralized network comprised of many smaller interconnected networks. Networks are largely comprised of end systems, referred to as hosts, and intermediate systems, called routers. Information travels through a network on one of many paths, which are selected through a routing process. Routing protocols communicate reach ability information (how to locate other hosts and routers) and ultimately perform path selection. BGP is an external protocol: it allows different autonomous systems to exchange routes. A network under the administrative control of a single organization is called an autonomous system (AS). There are two types of routing, intra-domain routing which is the process of routing within an AS, and interdomain routing which is the process of routing among different ASes. BGP runs in External BGP (eBGP), which is the protocol used to communicate between two autonomous systems, and Internal BGP (iBGP), which is the protocol that the AS uses to synchronize its own routing tables.

Do not confuse eBGP with EGP, a nearly obsolete protocol once used on the Internet. Also, do no confuse iBGP with an IGP such as OSPF. ISPs use iBGP to distribute BGP routes between routers within an AS. However, ISPs usually still need to run an IGP to generate routes for traffic within the AS.

On the ProCurve Secure Router, eBGP is intended to allow a private network to send and receive routes from remote sites through the Internet. The private network itself will run an IGP such as RIP or OSPF.

The WAN router runs BGP to communicate with the connecting ISP router, also called the ISP edge router. The ISP tunnels the routes advertised by the local router through the Internet to the remote sites. Only ISP routers that connect to routers at the private organization's remote sites can receive these routes, which they then pass to the private routers. Routers internal to the ISP run an internal routing protocol and do not receive the private routes.

1.1 Advantages

- BGP offers several advantages, particularly in more complex environments:
- Unlike routers using static routing, routers running BGP can automatically respond to downed connections and changes in network topology.
- Your organization can change its IP addressing without notifying your ISP.
- BGP can handle complex applications in which the private network connects to multiple ISP routers or multiple ISPs. You can configure BGP to balance loads among these connections.
- BGP is the native protocol run by ISPs, which decreases problems caused by redistributing static or RIP routes into BGP.

- BGP is policy based, so you maintain tight control over the routes transmitted and accepted.

1.2 Disadvantage

The main disadvantage in using BGP is that it requires you to purchase and run your own BGP router.

II. BASIC BGP CONFIGURATION

The first thing that must be understood is that each BGP device can have both internal and external BGP connections to other devices. Internal BGP connections are within the same AS while external BGP connections are between different AS's. This is important because the configuration and behavior is slightly different between the two.

2.1 eBGP Configuration

At its most basic the configuration of eBGP requires only two commands, these include:

- Router bgp *a*s-number
- Neighbor ip-address remote-as remote-as-number

What makes eBGP configuration obvious from iBGP configuration is that the AS-number which is used in the neighbor command is different than the AS-number configured with the router bgp command.

It must also be known that with eBGP by default there is a direct connection requirement which is enforced by an advertised TTL of 1. Now when configuring BGP using loopback interfaces this can become an issue as the packet actually takes two hops from the remote device to the physical interface and from the physical interface to the loopback interface. This issue can be resolved by using the neighbor ebgp-multihop command on Cisco equipment.

2.2 iBGP Configuration

iBGP configuration is very similar to eBGP configuration but requires a little understanding of iBGP requirements. By default, iBGP requires that all iBGP devices being used are fully meshed (although there are ways of getting around this). This does not however mean that a direct connection is required but that each iBGP peer must neighbor with each other iBGP router.

The following configuration shows that configuration of an iBGP neighbor is the same as with eBGP:

- Router bgp as-number
- Neighbor ip-address remote-as remote-as-number

The other thing that must be understood is how external BGP routes are advertised into iBGP.

The most common method of resolving this issue is by using the neighbor neighbor-ip-address next-hop-self command. When using this command the local eBGP peer will advertise the next-hop with its own IP address and not the address configured with the BGP neighbor command.

III. BGP ATTRIBUTES

Routes learned via BGP have associated properties that are used to determine the best route to a destination when multiple paths exist to a particular destination. These properties are referred to as BGP attributes, and an understanding of how BGP attributes influence route selection is required for the design of robust networks. This section describes the attributes that BGP uses in the route selection process:

- Weight
- Local preference
- Multi-exit discriminator
- Origin
- AS_path
- Next hop
- Community

3.1 Weight Attribute

Weight is a Cisco-defined attribute that is local to a router. The weight attribute is not advertised to neighboring routers. If the router learns about more than one route to the same destination, the route with the highest weight will be preferred.

3.2 Local Preference Attribute

The local preference attribute is used to prefer an exit point from the local autonomous system (AS). Unlike the weight attribute, the local preference attribute is propagated throughout the local AS. If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

3.3 Multi-Exit Discriminator Attribute

The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric.

The term suggestion is used because the external AS that is receiving the MEDs may be using other BGP attributes for route selection.

3.4 Origin Attribute

The origin attribute indicates how BGP learned about a particular route. The origin attribute can have one of three possible values

- ***IGP*** **-** The route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.
- ***EGP*** **-** The route is learned via the Exterior Border Gateway Protocol (EBGP).
- ***Incomplete*** **-** The origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP.

3.5 AS_path Attribute

When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed.

3.6 Next-Hop Attribute

The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers.

3.7 Community Attribute

The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. Predefined community attributes are listed here:

- ***No-export*** **-** Do not advertise this route to EBGP peers.
- ***No-advertise*** **-** Do not advertise this route to any peer.
- ***Internet*** **-** Advertise this route to the Internet community; all routers in the network belong to it.

IV. HOW DOES BGP WORKS

BGP uses TCP as the transport protocol, on port 179. Two BGP routers form a TCP connection between one another. These routers are peer routers. The peer routers exchange messages to open and confirm the connection parameters.

BGP routers exchange network reachability information. This information is mainly an indication of the full paths that a route must take in order to reach the destination network. The paths are BGP AS numbers. This information helps in the construction of a graph of ASs that are loop-free. The graph also shows where to apply routing policies in order to enforce some restrictions on the routing behavior.

Any two routers that form a TCP connection in order to exchange BGP routing information are "peers" or "neighbors". BGP peers initially exchange the full BGP routing tables. After this exchange, the peers send incremental updates as the routing table changes. BGP keeps a version number of the BGP table. The version number is the same for all the BGP peers. The version number changes whenever BGP updates the table with routing information changes. The send of keepalive packets ensures that the connection between the BGP peers is alive. Notification packets go out in response to errors or special conditions.

V. PROTOCOL OVERVIEW

Routers that run a BGP routing process are often referred to as BGP speakers. Pair of BGP-speaking routers that form a TCP connection to exchange routing information between them are called BGP neighbors or peers. A single router can participate in many peering sessions at any given time. Each BGP session takes place exactly between two nodes, where two routers exchange routing information dynamically, over TCP port 179.

For any two BGP peers in a network to be able to send and receive traffic with each other, all intermediate BGP routers have to forward traffic such that the packets get closer to the destination. Because there can be multiple paths to a given target, BGP routers use a routing table to store all known topology information about the network. Based on its routing table, each BGP router selects the best route to use for every known network destination.

That information is stored in a forwarding table together with the outgoing interface for the selected best path. 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. It is assumed that the transport connection will deliver all data and eventually close properly in case of an error notification.

There are four possible message types used with BGP, all consisting of a standard header plus specific packet-type contents.

- ***OPEN:*** First message to open a BGP session, transmitted when a link to a BGP neighbor comes up. It contains AS number (ASN) and IP address of the router who has sent the message.
- ***UPDATE:*** Message embracing routing information, including path attributes. It contains Network Layer Reachability Information (NLRI), listing IP addresses of new usable routes as well as routes that are no longer

active or viable and including both the lengths and attributes of the corresponding paths.

- ***NOTIFICATION:*** Final message transmitted on a link to a BGP neighbor before disconnecting. It usually describes atypical conditions prior to terminating the TCP connection, and provides a mechanism to gracefully close a connection between BGP peers.
- ***KEEP-ALIVE:*** Periodic message between BGP peers to inform neighbor that the connection is still viable by guaranteeing that the transmitter is still alive. It is an application type of message that is independent of the TCP keep-alive option.

The BGP protocol has four main stages:

1. Opening and confirming a BGP connection with a neighbor router. After two BGP peers establish a TCP connection, each one sends an OPEN message to the other.

2. Maintaining the BGP connection. A BGP router can detect a link or BGP peer host failure through the exchange of periodic keep-alive messages with the peer router. An error is assumed when no messages have been exchanged for the hold timer period. The hold timer period is calculated the smaller of its configured hold time setting and the hold time value received in the OPEN message. BGP utilizes periodic keep alive messages to ensure that the connection between neighbors does not time out.

3. Sending reachability information: Routing information is advertised between a pair of BGP neighbors in update messages. Each update message may simultaneously advertise a single feasible route to a neighbor and indicate withdrawal of several infeasible routes from service. Update messages contain NLRI with a list of <length, prefix> tuples designating reachable destinations, and path attributes, including degree of preference for each particular route.

4. Notifying error conditions: Notification messages are sent to a neighbor router when error conditions (incompatibility, configuration, etc.) are detected. Notification messages consist of a main error code and a more detailed sub-code.

VI. CONCLUSION

This paper described about loop free interdomain routing between autonomous using Border Gateway Protocol (BGP). BGP has been quite successful in providing relatively stable interdomain routing. BGP has been surprisingly robust. It was originally thought in many circles that the ISO's Interdomain Routing Protocol (IDRP) would be the successor to BGP, but because of diminishing interest in network protocols other than IP, BGP is the one interdomain routing alternative.

References

[1] Y. Rekhter, T. Li, S. Hares, "A Border Gateway Protocol 4 (BGP-4)", IETF, RFC 4271, January 2006.

[2] Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing", Proceedings of Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS'03), San Diego, California, USA. February2003.

[3] http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

[4] http://www.tcpipguide.com/free/t_TCPIPBorder Gateway Protocol BGP BGP4.html

[5] G. Sharma, L. Ragha ,"Hierarchical Origin and Path verification for securing inter-domain routing protocol", Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference

[6] L. Gao, "On inferring Autonomous System relationships in the Internet," IEEE/ACM Trans. Networking, vol. 9, no. 6, pp. 733-745, 2001.

[7] http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work

[8] http://en.wikipedia.org/wiki/Autonomous_system_ (Internet)M. Caesar and J. Rexford, "BGP Routing Policies in ISP Networks," Network, IEEE, vol. 19,no.6,pp.-11,2005.

[9] http://en.wikipedia.org/wiki/Border_Gateway Protocol