

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/299989244>

Implementation of Border Gateway Protocol (BGP) Attributes

Article · February 2016

CITATIONS

0

READS

127

2 authors:



Nael A. Zidan

Arab American University

8 PUBLICATIONS 0 CITATIONS

SEE PROFILE



Mohammad M. N. Hamarsheh

Arab American University

29 PUBLICATIONS 78 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Dynamic ocdma [View project](#)



successive interference cancellation [View project](#)

Implementation of Border Gateway Protocol (BGP) Attributes

Nae'l Zidan¹, Mohammad Hamarsheh²

¹Faculty of Graduate Studies, Arab American University-Jenin, Palestine

²Faculty of Engineering and information technology, Arab American University-Jenin, Palestine

ABSTRACT

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP implements routing policies based on a set of attributes accompanying each route used to choose the "shortest" path across multiple ASs. It also controlled by one or more routing policies. This paper describes implementation of BGP and BGP attributes using GNS3 and Cisco router Image. We include on this paper the comparative results for different BGP attributes implementation, in addition how these attributes affect routing path.

Keywords: BGP, BGP Attributes, BGP Attributes Implementation, GNS3

1. INTRODUCTION

Border Gateway Protocol (BGP) is the prevalent wide-area routing protocol, the internet composed of Autonomous System (AS's) that use BGP to implement inter-AS and intra-AS IP routing based on a set of attributes (Weight, Local preference, Multi-exit discriminator, Origin, AS_path, Next hop, Community). Routing involves two basic tasks, first task is determination of optimal routing paths, which is the complex, and the second is transport of information groups (Packets) through an internetwork, here we will use BGP to address the task of path determination.

BGP design motivated by three important goals, first one is scalability through dividing internet to AS under independent administration, the second is Policy in which AS has ability to implement and enforce various forms of routing policies, and the last one is cooperation under competitive circumstances in which the structure allow AS to determine among any set of choices.

AS which owned and administered by a single commercial entity, implements set of policies in deciding how to route its packets to the rest of Internet, and how to export its routes to other AS, and identified by a unique 16-bit number (the new is 32-bit number). Inside AS operates different routing protocols (Interior Gateway Protocols – IGP) which includes (RIP, OSPF, IS-IS, E-IGRP), and in contrast interdomain protocols like BGP are called Exterior Gateway Protocols (EGP).

Function of BGP System is to exchange reachability information including information about list of AS paths with other BGP systems. From this information it constructs AS connectivity graph so loops pruned and AS policy decisions enforced, each BGP router maintains a routing table that lists all feasible paths to a particular network, routing information received from peer routers is retained until an incremental update is received, BGP routers exchange routing information upon initial data exchange and after incremental updates, when an update occur routers send the portion of their routing table that has changed.

BGP protocol uses four message types. Open Message, which opens a BGP communications session between peers, open message is first message sent by each side after establishing of a transport-protocol connection. Update Message, which provide updates to other BGP systems, this message sent using TCP for reliable delivery and in this message the attributes for path (Origin, AS Path, Next Hop, Multiple-Exit Discriminator, Local Preference, etc.) included. Notification Message, which sent to describe an error that detected and used to close an active session. The last message is Keep-alive Message, which notify BGP peers that a device is active and sent often enough to keep the sessions from expiring [1], [2], [6].

2. BGP ATTRIBUTES

BGP path attributes categorized into four categories, well-known mandatory, well-known discretionary, optional

transitive, and optional non-transitive. Table 1 shows BGP attributes and their categories.

Well-known mandatory must recognize by all BGP implementation, and some of these attributes are mandatory and must include in each update message, others are discretionary (may or may not send in each update message).

Optional attributes, attributes that one or more may include in path, it is not required that all BGP implementation support all optional attributes. Transitive optional attributes may attach to the path by the originator or by any other BGP speaker in the path; he rules for attaching new non-transitive optional attributes will depend on the nature of the specific attribute. [6]

BGP attributes controlled by local AS administrator or by neighbor AS administrator, as shown in Table 1 some attributes and who control them.

Table 1: BGP Attributes

Attribute	Category	Controlled by Local AS / Neighbor AS
Origin	Well-known mandatory	Neither
Next Hop	Well-known mandatory	Local AS
AS Path	Well-known mandatory	Local AS
Local Preference	Well-known discretionary	Local AS
Atomic aggregate	Well-known discretionary	Neighbor AS
MED (Multi Exit Discriminator)	Optional non-transitive	Neighbor AS
Community	Optional transitive	Local AS
Aggregator	Optional transitive	Local AS

3. SIMULATION SETUP

For this simulation, we used GNS3 software, which offer an easy way to design and build networks of any size without the need of hardware [4], [5]. We used Cisco 7200 series routers IOS image.

For implementation, we used six Cisco 7200 series routers, two Virtual PC Shells (VPCS), connected with Gigabit Ethernet link as show on Figure 1.

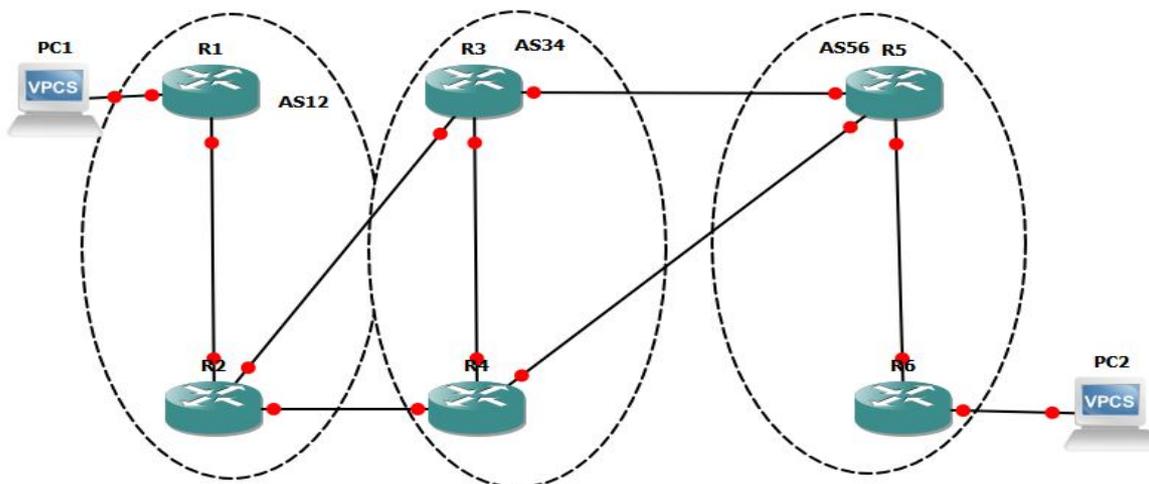


Figure 1 Network Topology [1]

3.1 Scenario 1: BGP without Policy

As shown in Figure 1, R1 & R2 Has AS12, R3 & R4 Has AS34, and R5 & R6 has AS56, each router has loopback interface which is always up with RIP protocol as shown on Table 2, each router loopback interface and RIP configuration.

Table 2: Routers Loopback Interface and RIP Configuration

Router	AS	Interfaces	RIP Conf.
R1	12	Loopback0: 192.0.5.1 GE2/0: 192.168.10.1/24	router rip version 2 network 192.0.5.0 network 192.168.1.0

R2	12	Loopback0: 192.0.2.1 GE1/0: 192.168.1.2/30 GE2/0: 192.0.4.2/30 GE3/0: 192.0.3.2/30	router rip version 2 network 192.0.2.0 network 192.168.1.0
R3	34	Loopback0: 192.0.10.1 GE1/0: 192.0.4.1/30 GE2/0: 192.168.2.1/30 GE3/0: 192.0.7.2/30	router rip version 2 network 192.0.10.0 network 192.168.2.0
R4	34	Loopback0: 192.0.8.1 GE1/0: 192.0.3.1/30 GE2/0: 192.168.2.2/30 GE3/0: 192.0.9.2/30	router rip version 2 network 192.0.8.0 network 192.168.2.0
R5	56	Loopback0: 192.0.14.1 GE1/0: 192.0.7.1/30 GE2/0: 192.0.9.1/30 GE3/0: 192.168.3.1/30	router rip version 2 network 192.0.14.0 network 192.168.3.0
R6	56	Loopback0: 192.0.12.1 GE1/0: 192.168.3.2/30 GE2/0: 192.168.20.1/24	router rip version 2 network 192.0.12.0 network 192.168.3.0

Two Virtual PC Shell (VPCS) used for testing reachability and routing path, PC1 connected to R1 with local subnet 192.168.10.0/24, IP address for PC1 is 192.168.10.100/24 and its gateway is 192.168.10.1 (R1 GE2/0 interface). PC2 connected to R6 with local subnet 192.168.20.0/24, IP address for PC2 is 192/168.20.100/24 and its gateway is 192.168.20.1/24 (R6 GE2/0 interface). BGP configuration including AS and neighbours as shown in Table 3.

Table 3: BGP Configuration

Router	AS	BGP Conf.
R1	12	router bgp 12 neighbor 192.0.2.1 remote-as 12 neighbor 192.0.2.1 update-source Loopback0
R2	12	router bgp 12 neighbor 192.0.3.1 remote-as 34 neighbor 192.0.4.1 remote-as 34 neighbor 192.0.5.1 remote-as 12 neighbor 192.0.5.1 update-source Loopback0
R3	34	router bgp 34 neighbor 192.0.4.2 remote-as 12 neighbor 192.0.7.1 remote-as 56 neighbor 192.0.8.1 remote-as 34 neighbor 192.0.8.1 update-source Loopback0
R4	34	router bgp 34 neighbor 192.0.3.2 remote-as 12 neighbor 192.0.9.1 remote-as 56 neighbor 192.0.10.1 remote-as 34 neighbor 192.0.10.1 update-source Loopback0
R5	56	router bgp 56 neighbor 192.0.7.2 remote-as 34 neighbor 192.0.9.2 remote-as 34 neighbor 192.0.12.1 remote-as 56 neighbor 192.0.12.1 update-source Loopback0
R6	56	router bgp 56 neighbor 192.0.14.1 remote-as 56 neighbor 192.0.14.1 update-source Loopback0 neighbor 192.168.3.1 remote-as 56

3.2 Scenario 2: BGP Policy with Local Preferences Attribute

We use same configuration in Scenario 1 with modification on BGP configuration for router 2, I add a route map for AS-Path that contains AS 56 will set a Local Reference attribute for neighbor (neighbour 192.0.3.1 remote-as 34) to 200, and leave local reference for others default value (100), configuration as following:

```
ip as-path access-list 1 permit _56_
route-map RM1 permit 10
match as-path 1
set local-preference 200

router bgp 12
address-family ipv4
neighbor 192.0.4.1 route-map RM1 in
```

3.3 Scenario 3: BGP Policy with AS-Path Prepend

We use same configuration in Scenario 1 with modification on BGP configuration for router 2, I add a route map for that prepend as-path, I duplicate the same AS three times so it appears has more and apply this route map to neighbour (neighbor 192.0.3.1 remote-as 34), configuration as following:

```
route-map RM1 permit 10
set as-path prepend 12 12 12

router bgp 12
address-family ipv4
neighbor 192.0.3.1 route-map RM1 in
```

3.4 Scenario 4: BGP Policy with Multi-Exit Discriminator (Metric) Attribute

We use same configuration in Scenario 1 with modification on BGP configuration for router 4, I add a route map for that set a Multi-Exit Discriminator (Metric) attribute for neighbor (neighbour 192.0.3.2 remote-as 12) to 200, and leave Metric for others default (0), configuration as following:

```
route-map RM1 permit 10
set metric 200

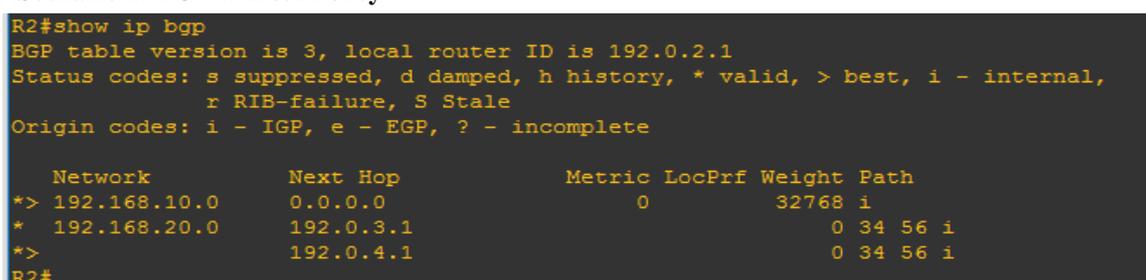
router bgp 34
address-family ipv4
neighbor 192.0.3.2 route-map RM1 out
```

3.5 Scenario 5: BGP Policy with Multi-Exit Discriminator (Metric) Attribute and Local Preferences Attribute

In this scenario, we merge route map configuration in scenario 2 and scenario 4, so the configuration on router (R4) set Metric in router (R2) for neighbor (neighbour 192.0.3.2 remote-as 12) to 200. Configuration of router (R2) set a Local Reference attribute for neighbor (neighbour 192.0.3.1 remote-as 34) to 200.

4 RESULTS DISCUSSION

4.1 Scenario 1: BGP without Policy



```
R2#show ip bgp
BGP table version is 3, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 192.168.10.0    0.0.0.0             0         32768 i
* 192.168.20.0    192.0.3.1           0         0 34 56 i
*> 192.0.4.1      192.0.4.1           0         0 34 56 i
R2#
```

Figure 2 R2 Routing Table

This results as show in Figure 2 routing table for router R2 without any policy it chooses the best routing from router 4 (192.0.4.1) for routing to AS 34 or AS 56.

Also same result when we apply a trace command from PC1 to PC2 as shown in Figure 3 the next hop after router R2 is also Router R4 (192.0.4.1).

4.2 BGP Policy with Local Preferences Attribute

```
R2#show ip bgp
BGP table version is 4, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 192.168.10.0   0.0.0.0             0         32768 i
*> 192.168.20.0   192.0.4.1          200        0 34 56 i
*                 192.0.3.1          100        0 34 56 i
R2#
```

Figure 3 R2 Routing Table

This results as show in Figure 3 routing table for router (R2) is changed since Local Preference for R3 (192.0.4.1) is 200 and others is 100, so the highest will be chosen, so R3 now chosen as a best route.

4.3 Scenario 3: BGP Policy with AS-Path Prepend

```
R2#show ip bgp
BGP table version is 3, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 192.168.10.0   0.0.0.0             0         32768 i
* 192.168.20.0    192.0.3.1          100        0 12 12 12 34 56 i
*>                192.0.4.1          200        0 34 56 i
R2#
```

Figure 4 R2 Routing Table

This results as show in Figure 4 routing table for router (R2) is changed since AS-Path route map prepend for R4 (192.0.3.1) is has more AS's, so the shortest AS-Path will be chosen, so R3 (192.0.4.1) now chosen as a best route.

4.4 Scenario 4: BGP Policy with Multi-Exit Discriminator (Metric) Attribute

```
R4#show ip bgp
BGP table version is 3, local router ID is 192.0.8.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
* i192.168.10.0   192.0.10.1          0         100      0 12 i
*>                192.0.3.2          0         100      0 12 i
* i192.168.20.0   192.0.10.1          0         100      0 56 i
*>                192.0.9.1          0         100      0 56 i
R4#
```

Figure 5 R4 Routing Table

```
R2#show ip bgp
BGP table version is 3, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 192.168.10.0   0.0.0.0             0         32768 i
* 192.168.20.0    192.0.3.1          200        0 34 56 i
*>                192.0.4.1          100        0 34 56 i
R2#
```

Figure 6 R2 Routing Table

This results as show in Figure 5 routing table for router (R4) which we change BGP configuration, but in its routing table will not be any modifications.

The changes as shown in Figure 6 which is a routing table for router (R2) and it is appear that metric for 192.0.3.1 is set to 200 (R4 map route), the lowest value of metric here will be chosen, so as shown router (R3 192.0.4.1) chosen, so R3 now chosen as a best route.

4.5 Scenario 5: BGP Policy with Multi-Exit Discriminator (Metric) Attribute and Local Preferences Attribute

```
R2#show ip bgp
BGP table version is 3, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.10.0     0.0.0.0            0         32768 i
* 192.168.20.0     192.0.4.1          0         34 56 i
*> 192.0.3.1       192.0.3.1          200        200      0 34 56 i
R2#
```

Figure 7 R2 Routing Table

From changes shown in Figure 7 (routing table for router R2), it is appearing that metric for 192.0.3.1 set to 200 (R4 map route), Local Preference set to 200 (R2 map route). Here priority for local preference, so higher local preference will choose for best route, as shown router (R4 192.0.3.1) chosen. R3 now chosen as a best route despite that router (R4) set a metric to 200 for interface going to router (R4).

5. CONCLUSION

BGP design accomplish its goal, with AS owner administration and enforcing policies. This simulation of BGP is mostly operation in real world is extremely complex. We discussed four route attributes, which are AS Path, Local Preference, Multi-Exit discriminator (Metric) and AS Path Prepend. In this simulation, we describe how to configure BGP, configure neighbors, how to configure setup of route map with different attributes and how to apply them.

References

- [1] Border Gateway Protocol (BGP): A Simulation Based Overview
- [2] Computer Networking A Top-Down Approach, James F. Kurose, Keith W. Ross
- [3] Matthew Caesar, Jennifer Rexford, "BGP routing policies in ISP networks", <http://www.cs.princeton.edu/~jrex/papers/policies.pdf>
- [4] <https://gns3.com/software>
- [5] <https://community.gns3.com/support/docs>
- [6] <http://tools.ietf.org/html/rfc4271>

AUTHORS

Nae'i Zidan received the B.S. in Computer Information Technology in 2005 from Arab American University Jenin (AAUJ), Palestine. He is a Master candidate of Computer Science at AAUJ, Palestine. He has 10+ years' experience of programming and development, networking, databases, and virtualization.

Mohammad M N Hamarsheh received his BS in electrical and computer engineering from An-najah National University, Nablus, Palestine, in 1999, and his MS and PhD degrees in computer and communication engineering and communications and network engineering, in 2002 and 2006, respectively from University Putra Malaysia, Serdang, Malaysia. He worked as the head of the FBG fabrication unit with Photronix, Cyberjaya, Malaysia. He was involved in optical CDMA and fiber Bragg grating research and development. He worked as a lecturer with faculty of information science and technology, Multimedia University, Malaysia, from 2005 to 2008. He is currently an assistant professor at Arab American University, Jenin, Palestine. His research interests include computer networking and security, optical code division multiple access systems, fiber Bragg gratings, dense wavelength division multiplexing, and polarization effect on optical fiber communication.