Border Gateway Protocol

It is an **interdomain routing protocol**, and it uses the **path-vector routing**. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

As we know that Border Gateway Protocol works on different autonomous systems, so we should know the history of BGP, types of autonomous systems, etc.

History of BGP

The first network was ARPANET, which the department of defense developed, and the Advanced Research Project Agency designed it. In Arpanet, only one network exists, which was handled by the single administrator. All the routers were the part of the single network, and the routing was performed with the help of the GGP (Gateway to Gateway Routing Protocol). The GGP was the first protocol among all the routing protocols. The autonomous system numbers were not used in the GGP protocol.

When the internet came into the market, then GGP started creating the problem. As the internet backbone became large due to which the routing table was also large, which led to the maintenance issue. To resolve this issue, the ARPANET was divided into multiple domains, known as autonomous systems. Each autonomous system can be handled individually, and each system has its own routing policy, and the autonomous system contains the small routing database. When the autonomous system concept was implemented, then the first routing protocol came known as RIP that runs on the single autonomous system. To connect the one autonomous system with another autonomous system, EGP (Exterior Gateway Protocol) protocol was developed. The EGP protocol was launched in 1984, defined in RFC 904. The EGP protocol was used for five years, but it had certain flaws due to which the new protocol known as Border Gateway Protocol (BGP) was developed in 1989, defined in RFC 1105.

There are many versions of BGP, such as:

- o   BGP version 1: This version was released in 1989 and is defined in RFC 1105.

- o   BGP version 2: It was defined in RFC 1163.

- o   BGP version 3: It was defined in RFC 1267.

- o   BGP version 4: It is the current version of BGP defined in RFC 1771.

BGP Autonomous Systems

BGP Autonomous Systems

RIP, IGRP,
EIGRP, OSPF

EGPs; BGP

Autonomous System 100

Autonomous System 200
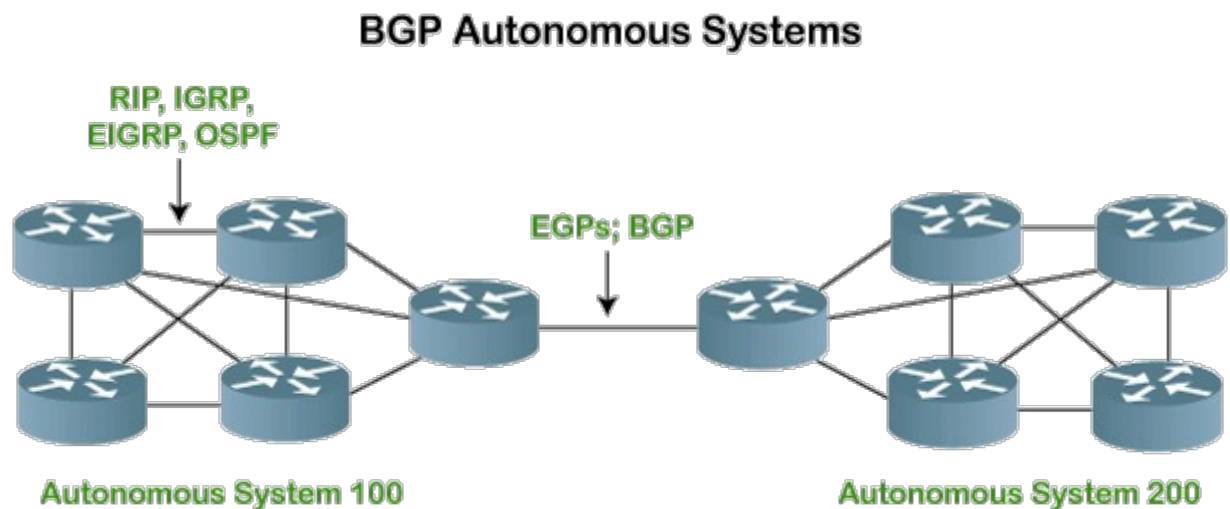
An autonomous system is a collection of networks that comes under the single common administrative domain. Or we can say that it is a collection of routers under the single administrative domain. For example, an organization can contain multiple routers having different locations, but the single autonomous number system will recognize them. Within the same autonomous system or same organization, we generally use IGP (Interior Gateway Protocol) protocols like RIP, IGRP, EIGRP, OSPF. Suppose we want to communicate between two autonomous systems. In that case, we use EGP (Exterior Gateway Protocols). The protocol that is running on the internet or used to communicate between two different autonomous number systems is known as BGP (Border Gateway Protocol). The BGP is the only protocol that is running on the internet backbone or used to exchange the routes between two different autonomous number systems. Internet service providers use the BGP protocol to control all the routing information.

BGP Features

The following are the features of a BGP protocol:

o **Open standard**

It is a standard protocol which can run on any window device.

o **Exterior Gateway Protocol**

It is an exterior gateway protocol that is used to exchange the routing information between two or more autonomous system numbers.

o **InterAS-domain routing**

It is specially designed for inter-domain routing, where interAS-domain routing means exchanging the routing information between two or more autonomous number system.

- o **Supports internet**

It is the only protocol that operates on the internet backbone.

- o **Classless**

It is a classless protocol.

- o **Incremental and trigger updates**

Like IGP, BGP also supports incremental and trigger updates.

- o **Path vector protocol**

The BGP is a path vector protocol. Here, path vector is a method of sending the routes along with routing information.

- o **Configure neighborhood relationship**

It sends updates to configure the neighborhood relationship manually. Suppose there are two routers R1 and R2. Then, R1 has to send the configure command saying that you are my neighbor. On the other side, R2 also has to send the configure command to R1, saying that R1 is a neighbor of R1. If both the configure commands match, then the neighborhood relationship will get developed between these two routers.

- o **Application layer protocol**

It is an application layer protocol and uses TCP protocol for reliability.
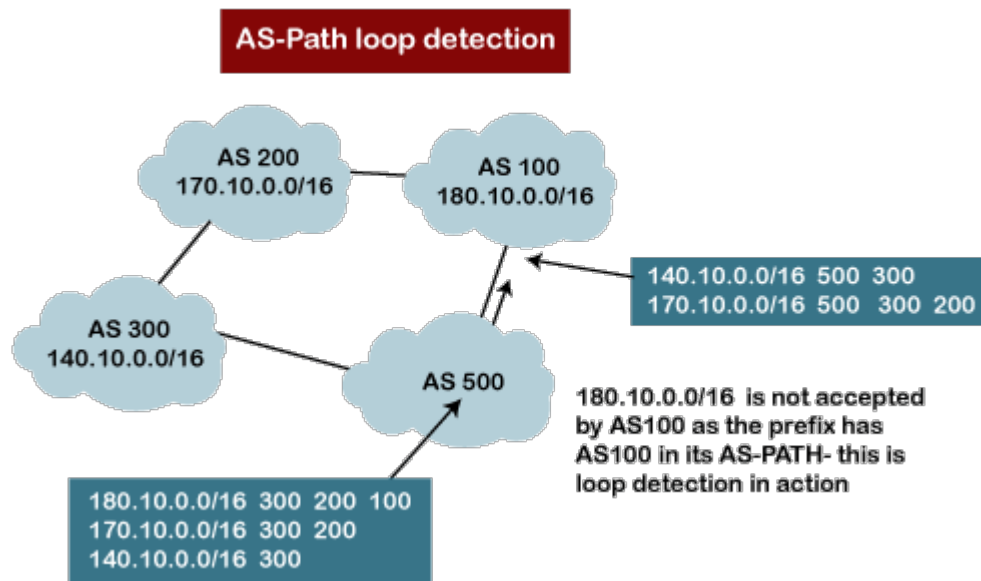
- o **Metric**

It has lots of attributes like weight attribute, origin, etc. BGP supports a very rich number of attributes that can affect the path manipulation process.

- o **Administrative distance**

If the information is coming from the external autonomous system, then it uses 20 administrative distance. If the information is coming from the same autonomous system, then it uses 200 administrative distance.

BGP's Loop prevention mechanism

BGP's loop prevention mechanism

AS-Path loop detection

AS 200
170.10.0.0/16

AS 100
180.10.0.0/16

140.10.0.0/16 500 300
170.10.0.0/16 500 300 200

AS 300
140.10.0.0/16

AS 500

180.10.0.0/16 is not accepted
by AS100 as the prefix has
AS100 in its AS-PATH- this is
loop detection in action

180.10.0.0/16 300 200 100
170.10.0.0/16 300 200
140.10.0.0/16 300

There is a possibility that when you are connecting to the internet, then you may be advertising route 10.0.0.0 to some autonomous system, then it is advertised to some other autonomous system. Then there is a possibility that the same route is coming back again. This creates a loop. But, in BGP, there is a rule that when the router sees its own AS number for example, as shown in the above figure, the network 180.10.0.0/16 is originating from the AS 100, and when it sends to the AS 200, it is going to carry its path information, i.e., 180.10.0.0/16 and AS 100. When AS 200 sends to the AS 300, AS 200 will send its path information 180.10.0.0/16 and AS path is 100 and then 200, which means that the route originates from AS 100, then reaches 200 and finally reaches to 300. When AS 300 sends to the AS 500, it will send the network information 180.10.0.0/16, and AS path is 100, 200, and then 300. If AS 500 sends to the AS 100, and AS 100 sees its own autonomous number inside the update, it will not accept it. In this way, BGP prevents the loop creation.
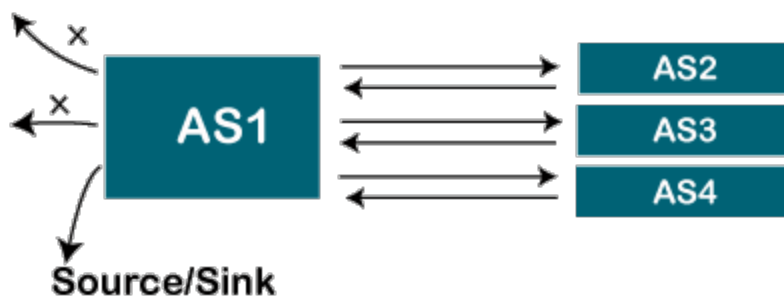
Types of Autonomous systems

The following are the types of autonomous systems:

o **Stub autonomous system**

Stub AS

Source/Sink
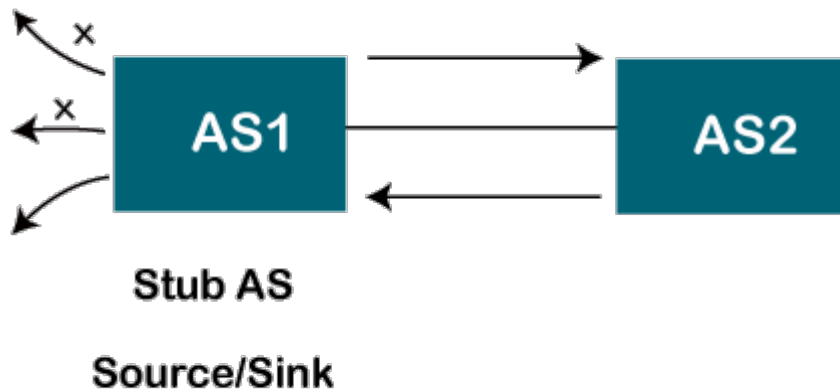
It is a system that contains only one connection from one autonomous system to another autonomous system. The data traffic cannot be passed through the stub autonomous system. The Stub AS can be either a source or a sink. If we have one autonomous system, i.e., AS1, then it will have a single connection to another autonomous system, AS2. The AS1 can act either as a source or a sink. If it acts as a source, then the data moves from AS1 to AS2. If AS1 acts as a sink, means that the data gets consumed in AS1 which is coming from AS2, but the data will not move forward from AS1.

    o **Multihomed autonomous system**

Source/Sink

It is an autonomous system that can have more than one connection to another autonomous system, but it can still be either a source or a sink for data traffic. There is no transient data traffic flow, which means that the data can be passed from one autonomous system.

   o **Transient Autonomous System**

The transient autonomous system is a multihomed autonomous system, but it also provides transient traffic flow.

Path attributes

The BGP chooses the best route based on the attributes of the path.

As we know that path-vector routing is used in the border gateway routing protocol, which contains the routing table that shows the path information. The path attributes provide the path information. The attributes that show or store the path information are known as path attributes. This list of attributes helps the receiving router to make a better decision while applying any policy. Let's see the different types of attributes. The path attribute is broadly classified into two categories:
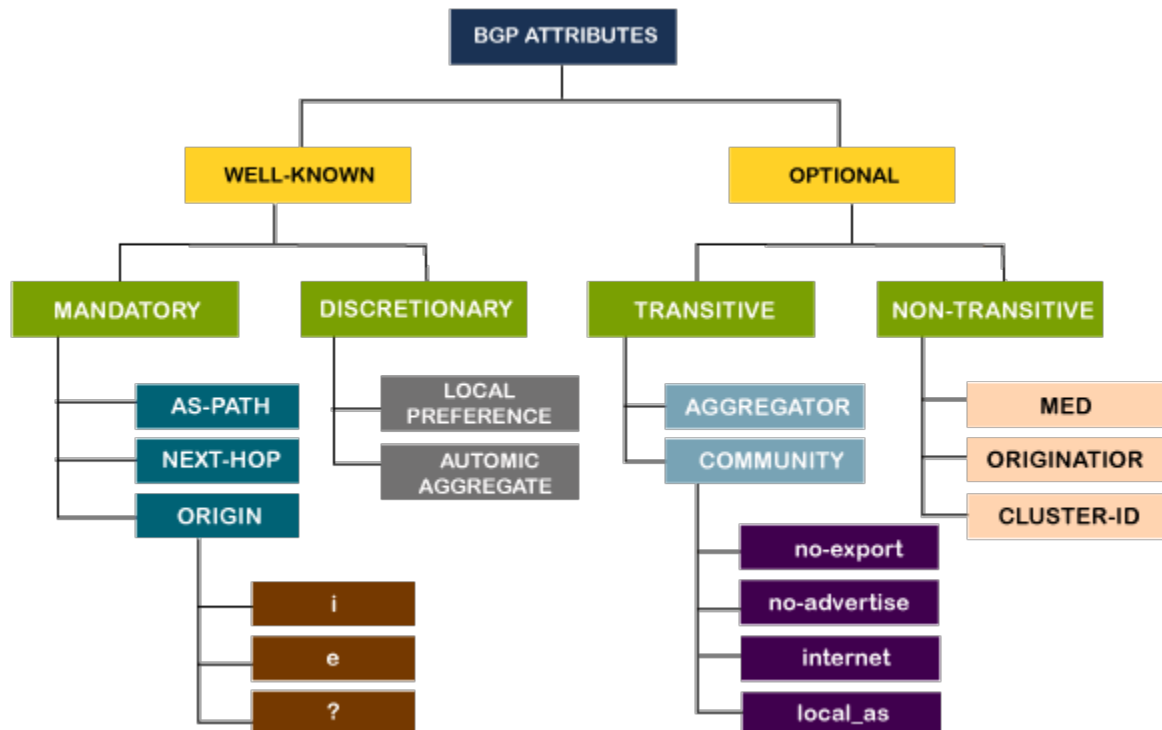
1. Well-known attribute: It is an attribute that should be recognized by every BGP router.

The well-known attribute is further classified into two categories:

- o **Well-known mandatory:** When BGP is going to advertise any network, but it also advertises extra information, and that information with path attributes information. The information includes AS path information, origin information, next-hop information. Here, mandatory means that it has to be present in all the BGP routing updates.
- o **Well-known discretionary:** It is recognized by all the BGP routers and passed on to other BGP routers, but it is not mandatory to be present in an update.

2. Optional attribute: It is an attribute that is not necessarily to be recognized by every BGP router. In short, we can say that it is not a mandatory attribute.

The optional attribute is further classified into two categories:

- o **Optional transitive:** BGP may or may not recognize this attribute, but it is passed on to the other BGP neighbors. Here, transitive means that if the attribute is not recognized, then it is marked as a partial.
- o **Optional non-transitive:** If the BGP cannot recognize the attribute, it ignores the update and does not advertise to another BGP router.
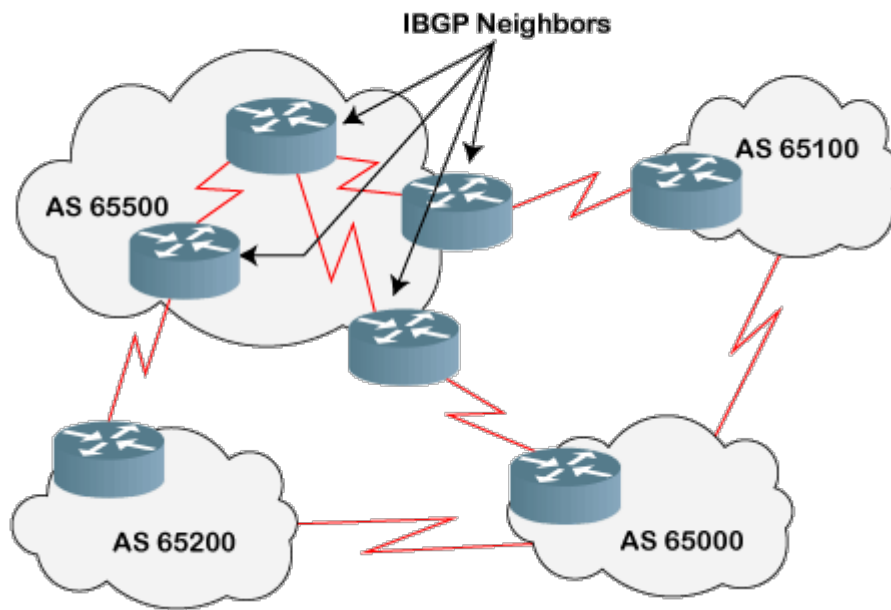
BGP Neighbors

BGP neighborship is similar to the OSPF neighborship, but there are few differences. BGP forms the neighboring relationship with the help of the TCP connection on port number 179 and then exchanges the BGP updates. They exchange the updates after forming the neighbor relationship. In BGP, the neighbor relationship is configured manually. BGP neighbors are also known as BGP peers or BGP speakers.
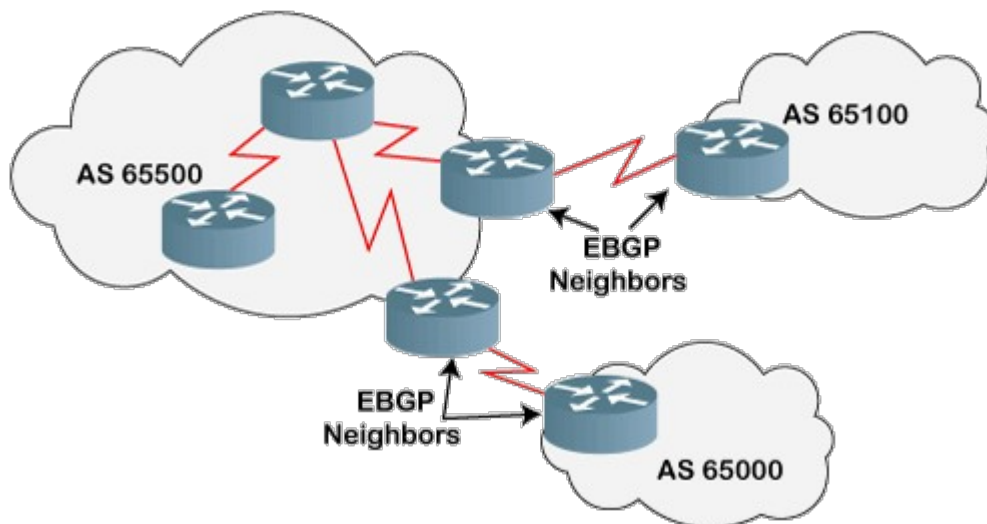
There are two types of neighbor relationship:

- o IBGP (Internal BGP): If all the routers are neighbors of each other and belong to the same autonomous number system, the routers are referred to as an IBGP.

IBGP neighbors

o EBGP (External BGP): If all the routers are neighbors of each other and they belong to the different autonomous number systems, then the routers are referred to as an EBGP.

EBGP neighbors

BGP Tables

There are three types of BGP tables:

o **Neighbor table:** It contains the neighbors who are configured by the administrator manually. The neighbor relationship has to be manually configured by using the neighbor command.

For the verification, the following commands are used:

1. #show ip bgp summary
2. # show ip bgp neighbors

The above commands are very useful to verify whether the neighbor relationship is up or not.

- o **BGP forwarding table:** It contains all the routes advertised in BGP and can be verified using the following command:

1. # show ip bgp

- o **IP routing table:** The IP routing table contains the best path routes required to reach the destination. The following command shows the best routing path:

1. #SH ip route

BGP Sessions

When we talk about the BGP, which means that the communication between the autonomous systems. Let's consider two autonomous systems having five nodes each.

BGP sessions are classified into two categories:

1. Internal BGP session

The internal BGP session is used to exchange information between the routers inside an autonomous system. In short, we can say that the routing information is exchanged between the routers of the same autonomous system.

2. External BGP session

The external BGP session is a session in which nodes or routers of different autonomous systems communicate with each other.

Types of packets

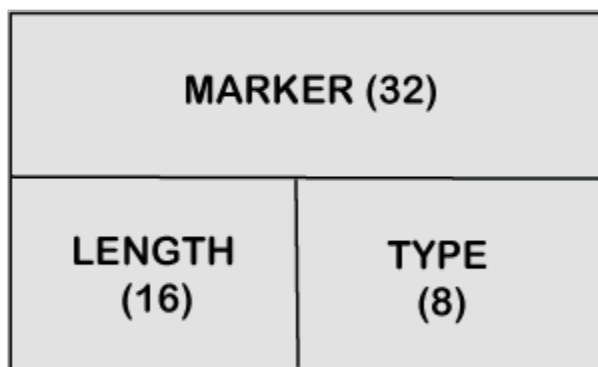**There are four different types of packets exist in BGP:**

- o **Open:** When the router wants to create a neighborhood relation with another router, it sends the Open packet.
- o **Update:** The update packet can be used in either of the two cases:

1. It can be used to withdraw the destination, which has been advertised previously.

2. It can also be used to announce the route to the new destination.

o   **Keep Alive:** The keep alive packet is exchanged regularly to tell other routers whether they are alive or not. For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.

o   **Notification:** The notification packet is sent when the router detects the error condition or close the connection.

BGP Packet Format

Now we will see the format in which the packet travels. The following are the fields in a BGP packet format:

BGP Packet Format

```
+-----------------------------------+
|                                   |
|           MARKER (32)             |
|                                   |
+----------------+------------------+
|                |                  |
|   LENGTH       |     TYPE         |
|    (16)        |      (8)         |
|                |                  |
+----------------+------------------+
```

1. **Marker:** It is a 32-bit field which is used for the authentication purpose.
2. **Length:** It is a 16-bit field that defines the total length of the message, including the header.
3. **Type:** It is an 8-bit field that defines the type of the packet.