“Global Routing Optimization using BGP”

Submitted August 2024, in partial fulfillment of
the conditions of the award of the degree MSc. Cybersecurity

Jash Vaidya

School of Computing and Engineering

University of West London

I hereby declare that this dissertation is all my own work, except as where specific references are made to the work of others (including AI):

Signature Jash Vaidya
Date 23/08/2024

Declaration

I, the undersigned, hereby state that the thesis entitled “Global Routing Optimization using BGP” submitted by me has been prepared without any help. I also state that the thesis has not been subject to procedures connected with acquiring an academic (Master’s) degree at a higher education institution at any earlier time.

Moreover, I declare that this version of the thesis is identical with the submitted electronic version.

Jash Vaidya
date author’s legible signature

I declare that this thesis has been prepared under my direction, and I state that it fulfills the conditions for presenting it in proceedings for acquiring an academic degree.

....
date Supervisor’s legible signature

Table of Contents

ACKNOWLEDGEMENT 5

ABSTRACT 6

FIGURE 7

TABLE 8

LIST OF ACRONYMS 9

CHAPTER 1 10

1 Introduction 10

1.1 introduction 10
1.2 Background 10
1.3 Statement of problem 11
1.4 Scope 11

CHAPTER 2 12

2 BGP Basics 12

2.1 Internal and External BGP 12
2.2 eBGP and iBGP 13
2.3 Autonomous System (AS) relationships and hierarchy 14
2.4 Impact of AS relationships on BGP operations 16
2.5 BGP Attributes 17
2.6 Model of BGP Routing 23
2.7 Decision Process 25

CHAPTER 3 28

3 Methodology 28

3.1 Approach 28
3.2 Tools for BGP Management 28

CHAPTER 4 32

4 BGP SCALING 32

4.1 BGP Route Refresh 32
4.2 BGP Confederation 34
4.3 BGP Messages 36
4.4 BGP Route Reflector 36

CHAPTER 5 38

5 Implementation...38
5.1 implementation...38
5.2 Flow-tag propagation...39

CHAPTER 6...40

Network Test...40
6.1 Detailed Verification Process for BGP Neighborship...40

CHAPTER 7...43

BGP Optimization...43
7.1 BGP Vulnerabilities...43
7.2 Cryptographically enhanced BGP...44
7.3 Temporal Cache Management Schemes...46

CHAPTER 8...48

Conclusion...48

BIBLIOGRAPHY...49

SUMMARY...51

Acknowledgement

The Completion of this Thesis could not have been possible without the expertise of **Dr. Shidrokh Goudarzi, Assistant Professor in Computer Science**, from the faculty of applied University of West London (UWL), UK.

Also, sincere appreciation and thanks to all other staff member of the University for the Level of education provided during this master’s course.

Last but not least, big thanks to my parents because of whom I made it till here, without their support this would indeed be impossible.

Abstract

The dissertation titled "Global Routing Optimization using BGP" by Jash Rajeshkumar Vaidya explores the Border Gateway Protocol (BGP), which is essential for routing data across the internet. It begins by emphasizing the importance of BGP in ensuring efficient and stable internet connectivity, especially as the web expands and the number of devices increases.

BGP operates as a path vector protocol, meaning it tracks routes based on destination and path details, rather than factors like speed or the number of hops. This makes it unique compared to other protocols. The document highlights two main types of BGP: internal BGP (iBGP), used within a single organization, and external BGP (eBGP), which connects different organizations. Each type has specific characteristics and requirements for managing routing information.

The dissertation also discusses the security enhancements in BGP, such as BGPsec, which helps prevent issues like route hijacking. It addresses the challenges organizations face in managing BGP, particularly in balancing performance and security. Large companies, like Google and Amazon, must continually optimize their BGP configurations to maintain efficient operations.

Additionally, the study looks at how BGP management can be integrated into broader organizational strategies, such as Project Portfolio Management (PPM). This integration is crucial for aligning technical capabilities with organizational goals, especially for non-profits that operate under tight budgets.

Overall, the dissertation aims to provide insights into effectively managing and optimizing BGP to meet the demands of modern networks while ensuring security and stability in the rapidly evolving digital landscape.

Figure

Figure 1 iBGP &eBGP 13
Figure 2 AS hierarchy 15
Figure 3 Local Preference 18
Figure 4 Origin 19
Figure 5 AS Path 19
Figure 6 Next Hop 20
Figure 7 MED (Multi Exit Discriminator) 21
Figure 8 Weight 22
Figure 9 Community 23
Figure 10 BGP Model 24
Figure 11 BGP States 27
Figure 12 Approach 28
Figure 13 Integration Flowchart 31
Figure 14 BGP Confederation 34
Figure 15 Route Reflector 37
Figure 16 Confederation and set of sub-AS 38
Figure 17 ACL Configuration (Arduino) 41
Figure 18 Configuring GTSM 41
Figure 19 Rate-Limiting Example (Python) 42

Table

Table 1 eBGP vs iBGP

List of Acronyms

AS – Autonomous System
BGP – Border Gateway Protocol
iBGP – Internal Border Gateway Protocol
eBGP – External Border Gateway Protocol
ISP – Internet Service Provider
sBGP – Secure Border Gateway Protocol
TCP – Transmission Control Protocol
TTL – Time to Live
MD5 – Message Digest algorithm 5
IP – Internet Protocol
PKI – Public Key Infrastructure
OSPF – Open Shortest Path First
IS-IS – Intermediate System to Intermediate System
RIP – Routing Information Protocol
IGP – Interior Gateway Protocol
EIGRP – Enhanced Interior Gateway Routing Protocol
IGRP – Interior Gateway Routing Protocol
ASN – Autonomous System Number
MED – Multi Exit Discriminator
3WHS –3 Way Handshake
FSM –Finite State Machine
WAN – Wide Area Networks
PHAS – Prefix Hijack Alert System
PSC – Prefix Sanity Checker
API – Application Programming Interface
SOR – System of RIB
EOR – End of RIB
RIB – Routing Information Base
RR – Route Reflector
IANA – Internet Assigned Numbers Authority
RIR – Regional Internet Registry
BBN – Bolt Beranek and Newman
IOS – Internetwork Operating System
DoS – Denial of Service

Chapter 1

1 Introduction

1.1 introduction

The rapid expansion of the World Wide Web necessitates enhanced stability and usability of the internet. Achieving this goal requires improving the efficiency and accessibility of the routing protocols that govern connections between routers. These routers exchange path information with their immediate neighbors and propagate it throughout the network, forming the overall network topology.

The Border Gateway Protocol (BGP) remains the primary external gateway routing protocol used to share routing information between autonomous systems (ASes) in the core network. As of 2024, BGP continues to be crucial for secure and efficient IP routing between these systems, effectively serving as the backbone of the Internet. Its inherent support for routing policies based on path characteristics ensures it remains the most suitable protocol for use between autonomous systems.

BGP, or Border Gateway Protocol, is known as a path vector protocol because it keeps track of routes by combining destination information with path details. It uses a specific method to choose the best route from multiple options based on these path details. This process doesn't consider factors like latency, connection usage, or the number of router hops. BGP is unique in its support for routing policies based on path characteristics, allowing the protocol to accept, reject, or modify routing information before making forwarding decisions. Other protocols like OSPF and IS-IS don't offer these capabilities, and while RIP does, it doesn't scale well for large networks. This makes BGP the only suitable protocol for routing between autonomous systems.

Recent advancements in BGP have focused on enhancing security and scalability to cope with the increasing complexity and size of the internet. For instance, BGPsec (BGP Security) has been developed to provide cryptographic validation of route announcements, helping to mitigate issues such as route hijacking and misconfigurations. Additionally, the adoption of technologies like Segment Routing over IPv6 (SRv6) is improving the flexibility and efficiency of BGP by enabling more straightforward and scalable traffic engineering.

The growth of the Internet of Things (IoT) and 5G networks has further underscored the importance of robust BGP mechanisms. These technologies rely on stable and scalable routing solutions to manage the vast number of devices and the significant increase in data traffic. Consequently, ongoing research and development efforts are aimed at ensuring BGP can handle these emerging demands while maintaining the security and stability of the global internet infrastructure.

1.2 Background

This dissertation addresses the full spectrum of BGP, from its fundamental principles to advanced techniques for managing and optimizing its performance. The study is not limited to theoretical discussions; it also includes practical aspects of BGP implementation and real-world challenges faced by organizations that rely on this protocol for their daily operations. For instance, large tech companies like Google and Amazon, which operate vast global networks, must continually optimize BGP to maintain high levels of performance and security. These companies face the ongoing challenge of balancing network efficiency with the need to protect against threats such as BGP hijacking.

In addition to examining how BGP functions and how it can be optimized, this dissertation also considers the implications of BGP management within the framework of Project Portfolio Management (PPM). While the primary focus is on BGP itself, understanding its role within PPM is crucial for organizations that need to align their networking strategies with broader organizational goals. For example, non-profit organizations often operate under tight budgets and must ensure that their network infrastructure is both cost-effective and reliable. Effective BGP management within PPM can lead to better resource allocation, improved project outcomes, and enhanced network security.

1.3 Statement of problem

The central problem this dissertation seeks to address is how to effectively manage and optimize BGP in a way that supports both the technical demands of modern networks and the strategic goals of organizations. This includes exploring the challenges of dynamic BGP adaptation in response to network changes, securing BGP against emerging threats, and integrating BGP management into broader organizational frameworks like PPM.

This study is inspired by the growing need for a comprehensive understanding of BGP, especially as the internet evolves and new challenges arise. By combining technical analysis with practical insights, the dissertation aims to provide a valuable resource for network administrators, IT professionals, and organizational leaders who need to manage and optimize BGP in a rapidly changing digital landscape.

The objectives of this dissertation are to thoroughly investigate the workings of BGP, explore advanced management and optimization techniques, and assess how these practices can be integrated into broader organizational strategies. Key research questions include: How can BGP be optimized for efficiency and security in large-scale networks? What are the best practices for managing BGP in different organizational contexts? And how can BGP management be aligned with Project Portfolio Management to support organizational goals?

1.4 Scope

The scope of this study encompasses both the technical and strategic aspects of BGP, with a focus on practical applications in real-world environments. While the primary emphasis is on BGP itself, the research also addresses its integration into organizational strategies, particularly in sectors where network efficiency and security are paramount.

Chapter 2

2 BGP Basics

2.1 Internal and External BGP

BGP, or Border Gateway Protocol, is the language routers use on the Internet to determine how data packets should travel from one router to another to reach their final destination. BGP has proven highly effective and continues to be essential for the functioning of the Internet. (cloudflare, n.d.)

BGP comes in two forms: iBGP (internal BGP) and eBGP (external BGP). Here's a brief overview of each:

1. **iBGP (Internal BGP)** iBGP is used within a single autonomous system (AS) to share routing information among internal routers. It requires a full mesh topology or the use of route reflectors and confederations to distribute prefix information. The default administrative distance for iBGP is 200. Routes learned from an iBGP neighbor are not advertised to other iBGP peers. Typically, the TTL (Time to Live) for iBGP neighbors is set to 255. iBGP is used within the same organization and employs BGP Split Horizon to prevent routing loops.
2. **eBGP (External BGP)** eBGP is used to exchange routing information between different autonomous systems. It is deployed on border routers that connect separate networks, such as those of different organizations or between an organization and an Internet Service Provider (ISP). The default administrative distance for eBGP is 20. A stub AS generally only runs EBGP on one or perhaps more edge routers and routes packets towards and through the edge routers by an IGP. By default, any route learned with an eBGP neighbour is published ahead to next IBGP or eBGP peer. TTL = 1 is the default setting for eBGP neighbours, implying that peers are regarded to be explicitly linked. It is generally deployed among two organizations or in between two organizations and an Internet Service Provider. eBGP utilizes AS PATH for avoiding loops.

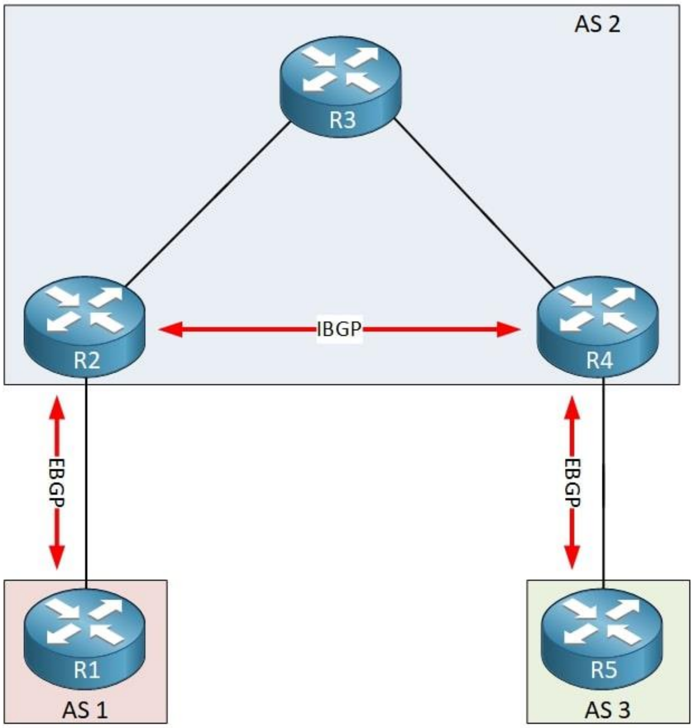


Figure 1 iBGP &eBGP

External BGP (eBGP) is used to exchange routes and transfer traffic across the Internet. Autonomous systems can also use an internal version of BGP, known as internal BGP (iBGP), to route traffic within their internal networks. It's important to note that using iBGP doesn't require the use of eBGP. Autonomous systems can use various internal protocols to connect the routers within their networks.

Although the core principles of the protocol are the same whether used as eBGP or iBGP, there are significant differences in how the two operate. An iBGP speaker does not forward routing information received from one iBGP peer to another iBGP peer to prevent routing loops. In contrast, eBGP uses the AS Path attribute to avoid loops.

2.2 eBGP and iBGP

SR.NO	EBGP	IBGP
1	EBGP stands for External Border Gateway Protocol.	IBGP stands for Internal Border Gateway Protocol.
2	It runs between two BGP routers in different autonomous system.	It runs between two BGP routers in the same autonomous system.

SR.NO	EBGP	IBGP
3	Its default Administrative Distance is 20.	Its default Administrative Distance is 200.
4	EBGP routes received from an EBGP peer can be advertised to EBGP and IBGP peers.	IBGP routes received from an IBGP peer cannot be advertised to another IBGP peer but can be advertised to an EBGP peer.
5	It does not require full mesh topology.	It requires full mesh topology.
6	It is used between organization or between organization and Internet Service provider.	It is used within the same organization.
7	It uses as path for loop prevention.	It uses BGP Split horizon for loop prevention.
8	It default peers are set with TTL = 1.	It default peers are set with TTL = 255.
9.	In EBGP peers, attributes like local preference are not sent.	In IBGP peers, attributes like local preference are sent.
10.	When route is advertised to EBGP peer, next hop is changed to local router .	When route is advertised to IBGP peer, next hop remains unchanged.

Table 1 eBGP vs iBGP (geeksforgeeks, n.d.)

2.3 Autonomous System (AS) relationships and hierarchy

Autonomous Systems provide a two-level Internet routing hierarchy. An Autonomous System (AS) is a collection of routers managed by a single administrator, where prefixes and routing policies are controlled. Routing between different ASes occurs externally and involves one AS sending traffic to another. Within an AS, routers use an Interior Gateway Protocol (IGP) to manage routing between networks inside the AS.

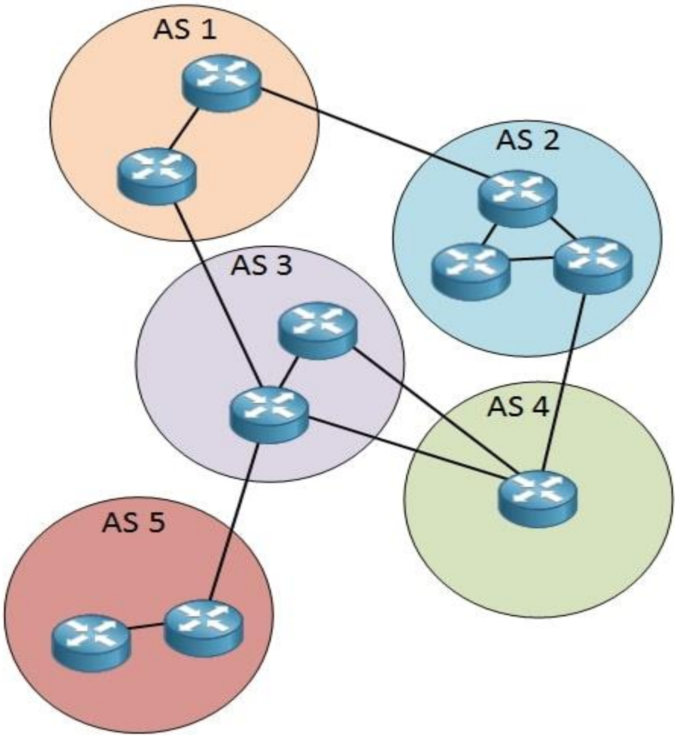


Figure 2 AS hierarchy

RIP, OSPF, IS-IS, EIGRP, and some private protocols like IGRP are popular interior gateway protocols. Routing within an Autonomous System (intra-AS routing) occurs internally and is not visible to external entities. All routers within an AS use the same intra-AS routing protocol. Specific gateway routers in each AS employ an inter-AS routing protocol to establish routing paths between different ASes. An Autonomous System needs a unique Autonomous System Number (ASN), a 32-bit identifier, if it shares routing information with other ASes on the internet. (inetdaemon, n.d.) The Internet Backbone is a network of large connections (routers and links) which connects huge autonomous systems, usually Tier 1 nodes. It is a distributed infrastructure, similar to the Internet that is maintained by a number of businesses, universities, and other organizations.

Categories of Autonomous Systems

1) Stub Autonomous System
   This AS is only linked to one certain AS. A network which is linked to an AS is assigned the same AS number as the AS to which it is linked.

2) Transit Autonomous System
   This AS is linked to many other ASs and can be required to transport traffic among autonomous systems. These are mostly managed by major Internet service providers (ISPs).

3) Multi-Stub Autonomous System
   This is a network of one or many prefixes connecting to more than just a single service provider or we can say more than one AS.

2.4 Impact of AS relationships on BGP operations

To understand how real-world relationships impact the Border Gateway Protocol (BGP) routing protocol, let's consider the following scenario involving two internet service providers (ISPs):

Scenario: Peering and Transit Relationships

Companies Involved:

- **ISP A**: A large ISP with a global network.
- **ISP B**: A smaller regional ISP.
- **ISP C**: Another large ISP with a global network.
- **Company X**: A content provider, such as a streaming service, connected to ISP B.
- **End-User Y**: A user connected to ISP C who wants to access content from Company X.

BGP and Relationships

1. **Peering Relationship:**
    - **ISP A** and **ISP C** have a **peering relationship**. This means they exchange traffic between their networks for free, without charging each other. Peering relationships typically occur between ISPs of similar size and are intended to benefit both parties by reducing costs and improving performance.
    - **Impact on BGP**: In BGP, when ISPs A and C peer, they announce to each other the prefixes (IP address ranges) they manage. This enables traffic between these networks to be routed directly without needing a third party.
2. **Transit Relationship:**
    - **ISP B** has a **transit relationship** with **ISP A**. In this scenario, ISP B pays ISP A to carry its traffic to the rest of the internet. This relationship is typically between a smaller ISP (ISP B) and a larger ISP (ISP A) that has broader connectivity.
    - **Impact on BGP**: ISP A will announce ISP B's prefixes to the broader internet, allowing traffic from anywhere on the internet to reach ISP B's network. ISP B, in turn, will prefer to send traffic destined for the wider internet through ISP A.

Impact on Routing Decisions

Real-World Impact:

- **Traffic Flow from End-User Y to Company X:**
    - **Case 1**: If ISP C has a direct peering relationship with ISP B (which it doesn't in this example), traffic would flow directly from ISP C to ISP B, ensuring lower latency and fewer hops.
    - **Case 2**: Since ISP C and ISP B don't have a direct peering relationship, traffic from End-User Y in ISP C’s network must take an alternative path. In this case, the traffic could flow through ISP A, because of ISP B's transit agreement with ISP A. The path might be **ISP C → ISP A → ISP B → Company X**.
- **BGP Routing Decisions**:

    - BGP will determine the best path based on the **AS_PATH** attribute (among others). In this case, the path might be longer and could involve more hops, which might impact performance (e.g., increased latency for End-User Y accessing Company X's content).
- **Network Congestion and Costs**:
    - If ISP A and ISP C's peering link becomes congested or ISP A raises transit costs, ISP B might seek to establish a direct peering relationship with ISP C to avoid paying transit costs and improve performance.
    - This would lead to BGP route changes, where traffic from ISP B to ISP C would no longer need to pass through ISP A, leading to potentially shorter, more efficient routes.

2.5 BGP Attributes

The BGP attributes are the parts of BGP updates, which describes the characteristics of the prefix value. Some of them are mandatory while some are transitive or non-transitive.

2.5.1 Local Preference –

- The local preference attribute determines which route should be taken to quit the AS.
- It is a well deferred property which is utilized amongst iBGP peers but not sent on to external BGP neighbors.
- Within an autonomous structure, the Local Preference is used and shared between iBGP routers.

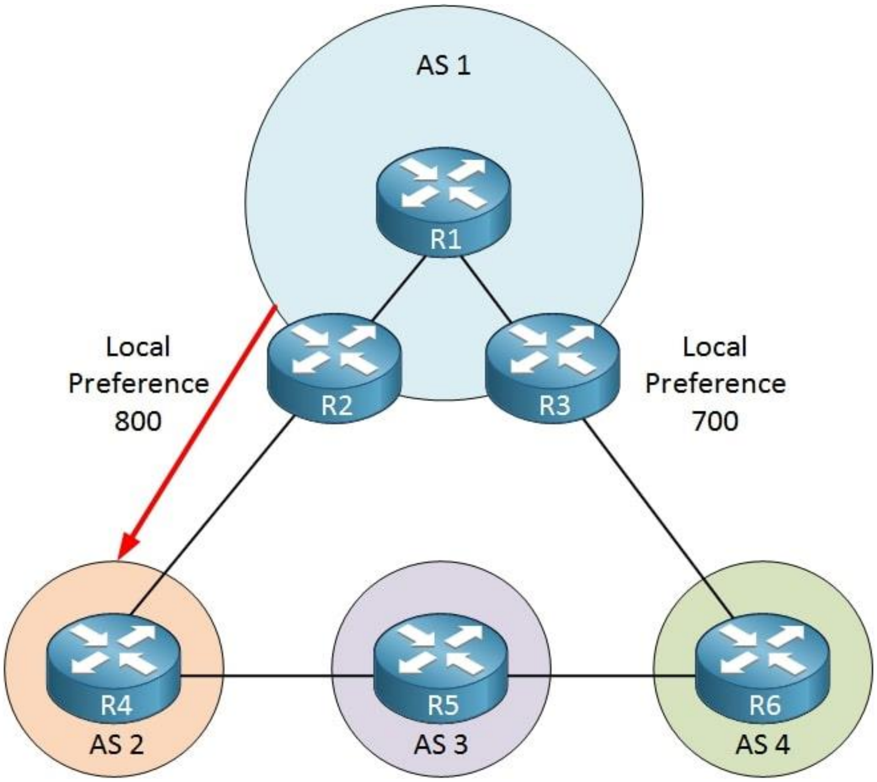
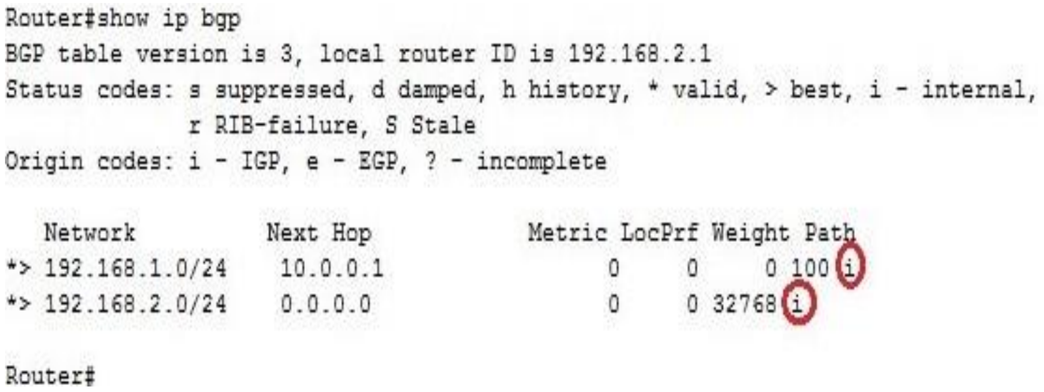


Figure 3 Local Preference

- On the BGP router, a default local preference is setup via an outbound connection.
- It subsequently broadcasts its local preference towards its inner iBGP neighbors.
- The most suitable paths are those with the greatest preference value.
- The default local preference is 100, and the greater the local preference, the better.

2.5.2 Origin –

- It is a well-known and also mandatory attribute.
- The origin attribute tells other autonomous systems about how the BGP prefix was implemented.
- A route in the BGP table can be obtained via the BGP network command, aggregation, or redistribution.
- IGP (i), EGP (e) and Incomplete (?) are the three different Origin type.



```
Router#show ip bgp
BGP table version is 3, local router ID is 192.168.2.1
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
*> 192.168.1.0/24   10.0.0.1                 0      0      0 100 i
*> 192.168.2.0/24   0.0.0.0                  0      0 32768 i

Router#
```

Figure 4 Origin

- With the "show ip bgp" command, we can see the BGP Origin Attribute information of any BGP Route. The Origin symbols (i, e or?) is displayed at the bottom of the output row.

2.5.3 AS path –

- This attribute is mainly used for Loop detection and also, Path metrics in which the distance of the AS Path is used to pick a path.
- This attribute identifies the autonomous systems by which routing information included in the Update message has traversed.
- When a route is advertised through one AS towards another, the AS PATH attribute is updated for each transmitted AS number, letting the recipient to know which ASs to route the message back to.

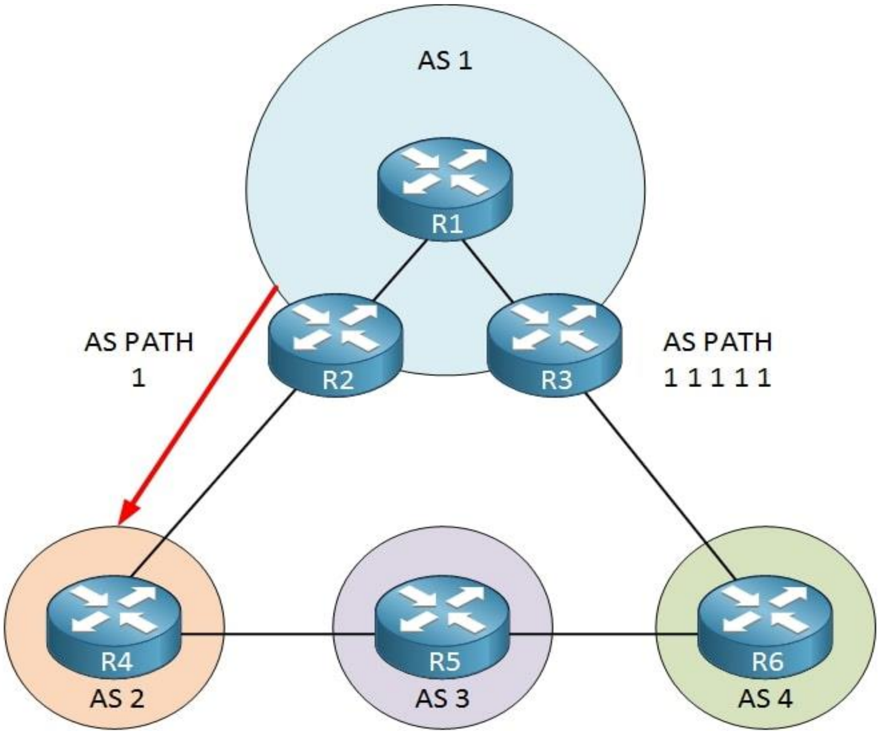


Figure 5 AS Path

- In certain cases, we may use a routing policy to manage BGP route selection by changing the AS PATH length.

- We may filter routes according to the AS numbers in the AS PATH attribute by setting an AS path filter lists.
- The AS PATH attribute may be used to identify and filter connections. (training.apnic, n.d.)

2.5.4 Next Hop –

- It is a well-known and mandatory attribute.
- Next-hop is the iBGP router’s loopback address
- Unlike IGP, the NEXT HOP attribute does not have to be an IP address of a physically linked router. (networklessons, n.d.)

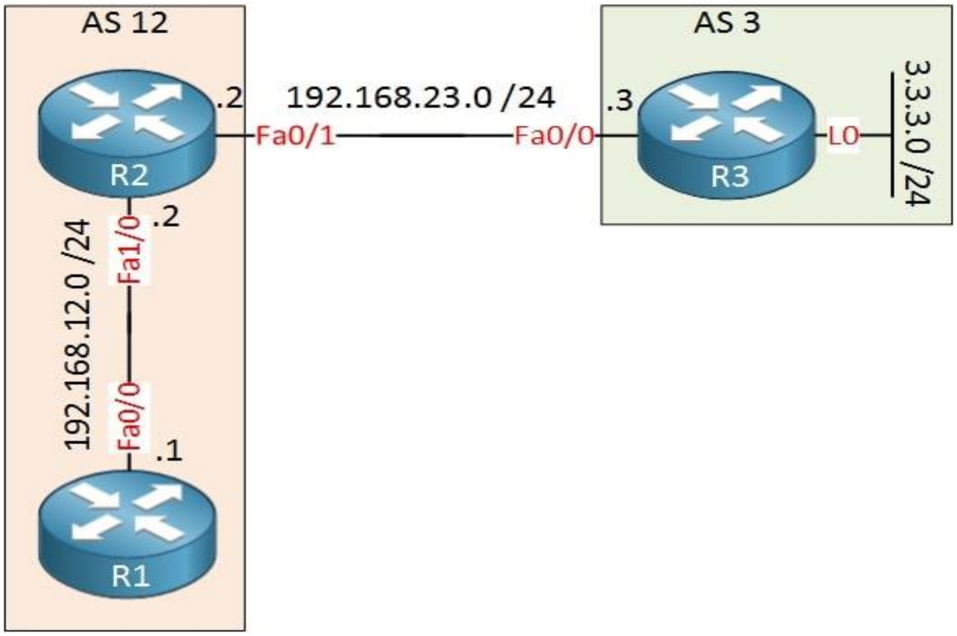


Figure 6 Next Hop

- When a BGP speaker advertises an inner route to an eBGP peer, it sets the NEXT HOP for such route to the address of its transmitting link.
- If load balancing is enabled, the NEXT HOP attribute gets altered.
- It allows IGP to make intelligent forwarding decision

2.5.5 MED (Multi Exit Discriminator) –

- MED can be only sent to EBGP neighbors.
- The MED attribute is transferred among two nearby ASs, none of which advertises it to any other AS.

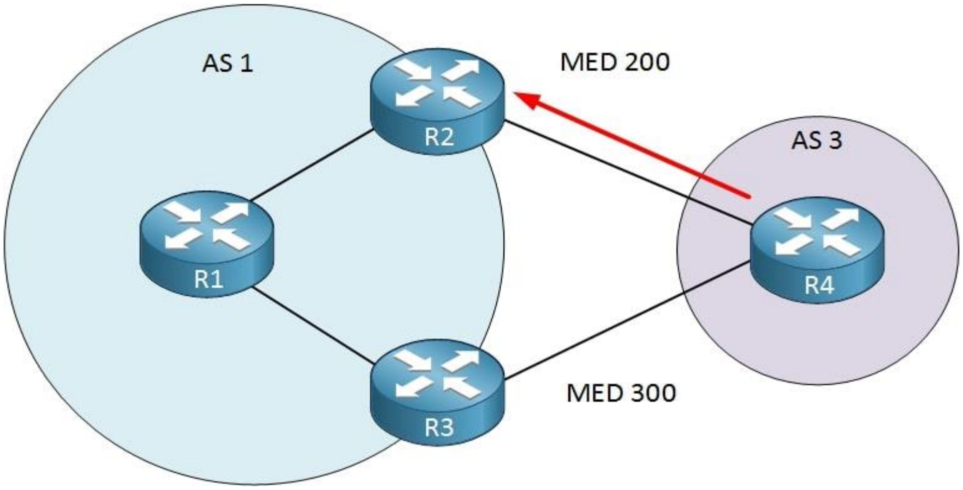


Figure 7 MED (Multi Exit Discriminator)

- MED, like IGP measurements, is used to identify the optimal path for traffic entering an AS.
- Lowest MED value are seen to be more desirable.
- When a BGP router receives several routes to a certain address with distinct next hops, it determines the route with lowest MED value to be the optimal route when all other parameters are matched.
- This attribute is non-transitive and also is optional. (catchpoint, n.d.)

Real world example:

Let's consider a scenario involving two major Internet Service Providers (ISPs) in the United Kingdom: **BT Group** and **Virgin Media**.

Scenario:
BT Group operates its network across the UK, with major data centres in London and Manchester. Virgin Media, another large ISP, also has a nationwide network, and they exchange traffic with BT at multiple interconnection points across the UK, including in London and Manchester.

Situation:
Virgin Media has customers distributed across the UK. To optimize network performance, BT wants traffic from Virgin Media destined for customers in the southern part of the UK (e.g., London, Brighton, Southampton) to enter BT's network through the London interconnection point. Similarly, traffic destined for the northern regions (e.g., Manchester, Liverpool, Leeds) should enter through the Manchester interconnection point.

Using MED:
To achieve this, BT sets a lower MED value for the routes it advertises to Virgin Media for traffic entering through London when the destination is in the southern UK. For routes entering through Manchester, BT sets a lower MED for destinations in the northern UK.

For each region, the MED values are set such that Virgin Media understands the preferred entry points into BT's network.
For example, BT might advertise a MED value of **10** for routes through London for southern destinations and a MED value of **20** for the same routes through Manchester. Conversely, for northern destinations, BT might advertise a MED value of **10** for Manchester and **20** for London.

Result:
Virgin Media's routers, when choosing the best path to forward traffic to BT's customers, will prefer to send traffic destined for southern cities through the London interconnection and northern traffic through Manchester, in line with the MED values set by BT. (techuk, n.d.)

2.5.6 Weight –

- Weight is allocated directly on a network to designate a preferable route out of a router for a recipient if several pathways present.
- Individual routes can have weights assigned to them, or all route received from a neighbor can have weights added to them.
- Highest weight of the path is most preferred.

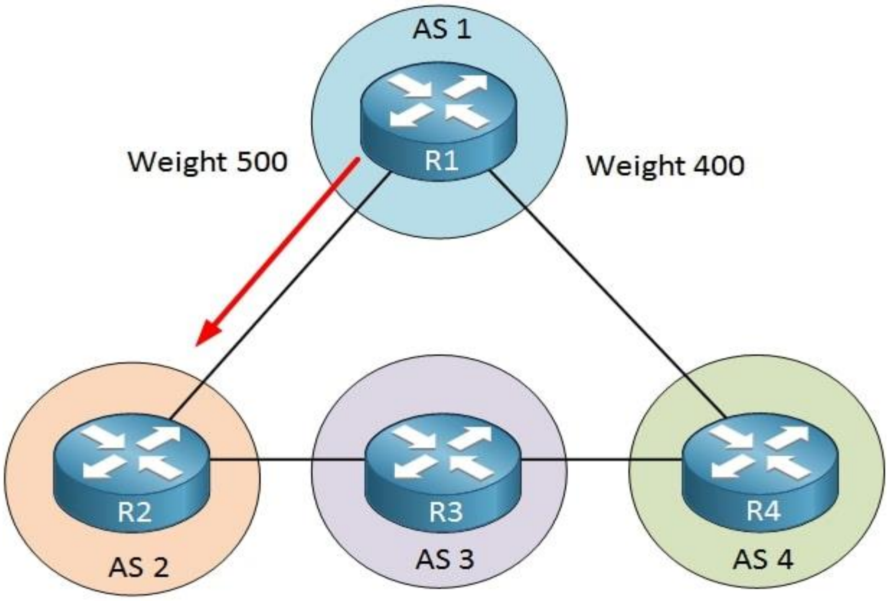


Figure 8 Weight

- We can use the weight rather than local preferences to affect the preferred path for external BGP neighbors.
- The value of the weight varies from 0 to 65,535.
- On the routes based filters, weight is assigned.

2.5.7 Community –

- The COMMUNITY attribute is designed to enhance routing policy utilization easier, as well as to make management and maintenance easier.

- This attribute defines a set of destination locations with similar properties which are segregated by physical boundaries and have nothing to do with the local AS.
- It might be as simple as choosing whether or not a prefix can indeed be transmitted, or as complex as impacting other BGP properties such as the AS_PATH or the LOCAL_PREF. It is even feasible to link the action with an informative tag in order to identify a much more precise result.
- There are well known Community attributes like Internet, No_Export, No_Advertise and No_Export_Subconfed.

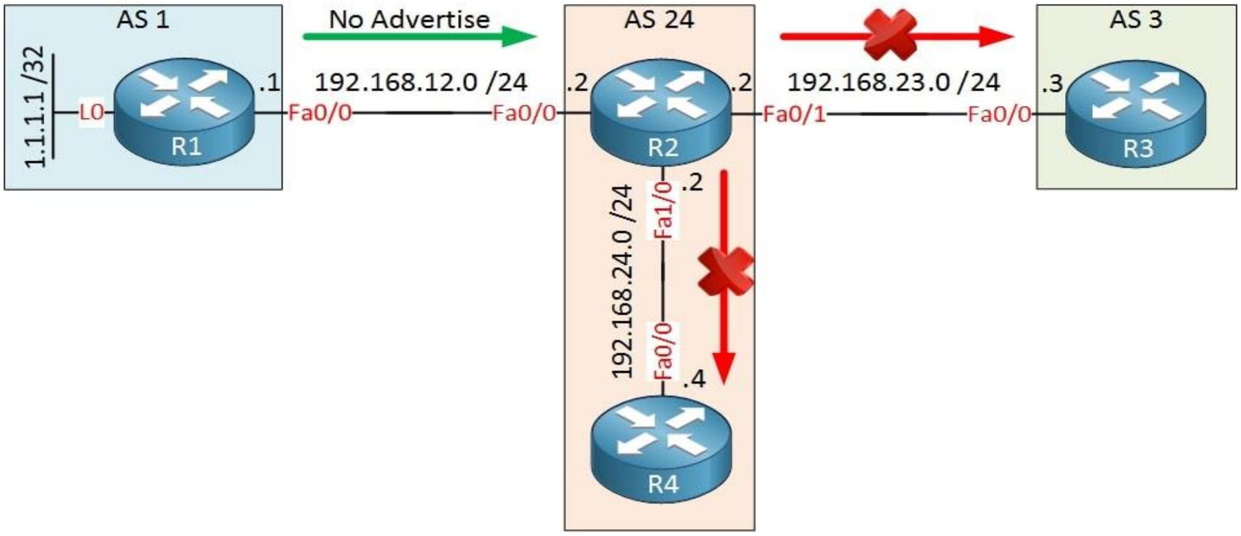


Figure 9 Community

- Internet - All routes are owned by the Internet community by design. The said attribute allows routes to be broadcast to all BGP neighbors.
- No_Export - Routes with such a characteristic can be published outside the local AS after they have been processed. The diagram below illustrates how advertisements reach each network in AS2 but are not transmitted to AS3.
- No_Advertise - Routes with this characteristic cannot be broadcast to additional BGP peers once they have been received.
- No_Export_Subconfed - Routes with this characteristic cannot be published outside the local AS after they have been obtained. (networklessons, n.d.)

2.6 Model of BGP Routing

Setting up routers manually involves establishing BGP neighbors, known as peers, to open a TCP session. To maintain the connection, a BGP speaker sends a 19-byte keep-alive message every 60 seconds. BGP is one of the few routing protocols that uses TCP as its transport protocol. BGP implementations continuously update routing tables to reflect real network changes, such as broken connections being restored or routers going down and coming back up.

Because of the limitations in BGP path selection, balancing inbound traffic to a multi-homed network across various routes can be challenging. One solution is to split a large IP address block into smaller blocks and adjust the route announcements so that different blocks are preferred on different routes. (networklessons, n.d.)

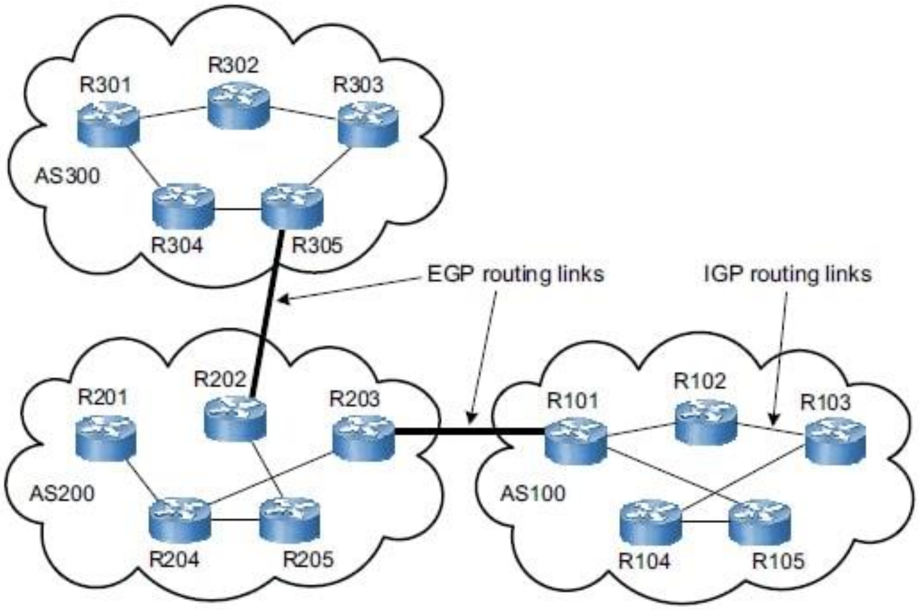


Figure 10 BGP Model

2.6.1 Real-World Application: Setting Up BGP Routers and Challenges

Setting up BGP routers involves navigating several challenges, particularly when it comes to inbound traffic balancing. This becomes critical when an autonomous system (AS) has multiple entry points, and effective traffic distribution is essential for optimal performance.

Example: Reliance Jio and Airtel

In India, Reliance Jio and Airtel are two major ISPs that exchange traffic across multiple interconnection points. Reliance Jio, with its extensive network infrastructure, has data centers in key cities like Mumbai and Delhi. Airtel, also with a significant presence, connects with Jio at several locations, including these major cities.

For instance, Reliance Jio might prefer that traffic destined for its southern India customers (e.g., Chennai, Hyderabad) enters through its data center in Mumbai, while traffic for northern India customers (e.g., Delhi, Noida) should enter through its data center in Delhi. To manage this, Jio uses the Multi Exit Discriminator (MED) attribute in BGP to influence the routing decisions of Airtel.

By advertising a lower MED value for routes entering through Mumbai for southern destinations, and a higher MED for routes entering through Delhi, Reliance Jio guides Airtel's routers to choose the optimal entry points based on geographic location. This approach helps balance the traffic load and reduces latency for end-users across different regions of India.

2.6.2 Small vs. Commercial Routers

The implementation of BGP can differ significantly between small networks and large-scale commercial environments.

Small Home or Business Routers

Small home or business routers in India, such as those used by small enterprises or residential users, generally do not employ BGP. These routers typically connect to the internet through a single ISP and use simpler routing protocols like RIP or OSPF. For example, a small office using a local ISP would rely on these basic protocols for internal traffic management.

Commercial Routers

On the other hand, commercial routers used by major ISPs like Reliance Jio and Airtel must support BGP to handle the complexities of large-scale networks. These routers are configured to manage multiple BGP sessions, extensive routing tables, and sophisticated policies such as MED to optimize routing and traffic distribution. For example, Airtel's routers must handle BGP configurations to efficiently manage traffic exchanges with Jio and other ISPs, ensuring effective load balancing and performance across its network.

2.7 Decision Process

BGP takes routing decisions based on routes, networking rules, as well as policy that a network administrator has configured. The BGP peer utilizes a straightforward finite state machine (FSM) with six states:

1. Idle
    - Refuses BGP incoming connections
    - Begins the event trigger setup process
    - Establishes a TCP connection with the configured BGP peer.
    - Waits for its peer to establish a TCP connection.
    - Its status is changed to Connected.
    - If an error appears at a certain point throughout the FSM operation, the BGP connection is instantly stopped and reverted to Idle mode

2. Connect
    - Waits for the TCP negotiation with the peer to be successful.
    - BGP first waits for the 3WHS to finish. When the operation is complete, the OPEN message is delivered to the neighbor, and BGP enters the OpenSent state.
    - If the TCP session has been successfully established, BGP does not spend enough time in this state.
    - Sends an Open signal to a neighbor and sets the status to OpenSent.

3. Active

- If the router is unsuccessful to create a successful TCP session, it becomes Active.
- BGP FSM attempts to re-establish a TCP session with the peer and, if succeeded, transmits an Open message to the neighbor.
- BGP switches to the Connect status when the ConnectRetry timeout is reset.
- If it fails again, the FSM is returned to the Idle state.

4. OpenSent
   - BGP FSM monitors its neighbor for an Open message.
   - BGP then waits for its neighbor to send an OPEN message. When received, BGP enters the OpenConfirm mode.
   - After receiving, the response the router verifies the Open message's authenticity.
   - If no errors occur, a Keepalive message is delivered, timers are established, and the status is changed to OpenConfirm.
   - If indeed the BGP process is restarted, we might return to an Idle mode.

5. OpenConfirm
   - The peer is going to wait for its peer to send a Keepalive message.
   - If a timer expires without receiving a Keepalive message, or if an error state occurs, the router returns to the Idle state.
   - Hence, BGP further continue to transmit keepalive notifications.

6. Established
   - In this state, the neighbors share information of each routes published to the BGP peer by sending Update messages.
   - If an error occurs in the Update message, a Notification message is delivered to the peer, and BGP returns to the Idle state.
   - The hold timer will indeed be restored whenever we get a keepalive or update notification.

A BGP implementation maintains a state object for each peer-to-peer session, tracking which of the six stages the session is currently in. The BGP protocol defines the messages that each peer must exchange to move the connection from one state to the next. Additionally, it specifies the updates that each peer must share to transition the session between states. (networklessons, n.d.)

Below is the figure for better understanding the BGP states/modes:

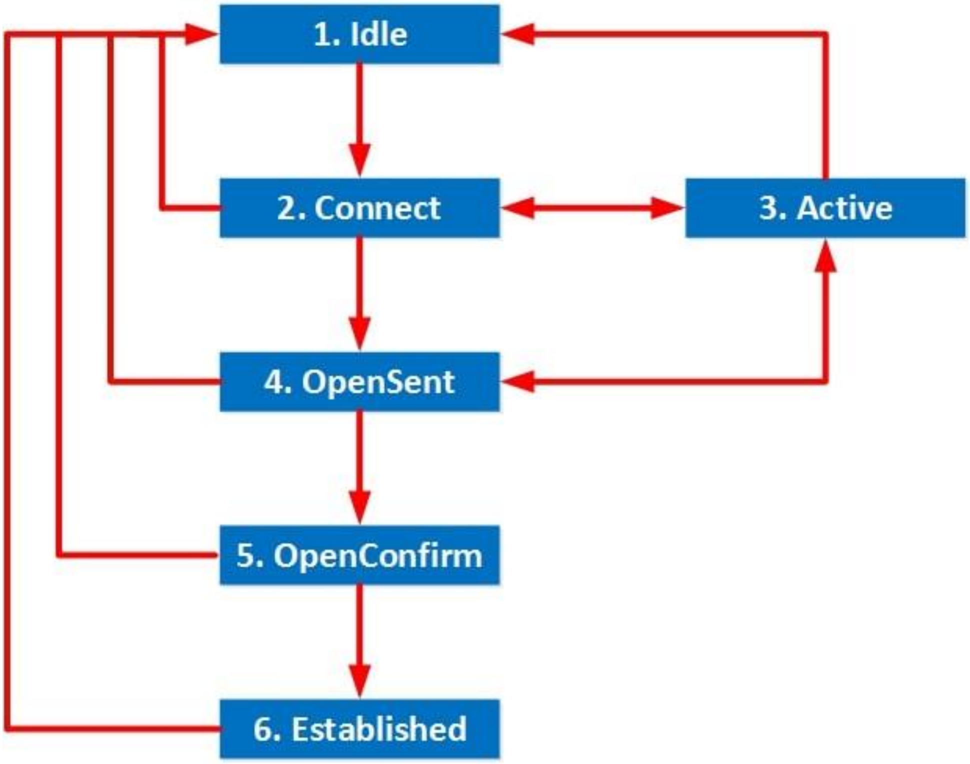


Figure 11 BGP States

Chapter 3

3 Methodology

3.1 Approach

Internet delay is primarily influenced by the distance packets travel on WAN networks. Reducing the number of hops between autonomous systems can decrease this delay. The main function of the BGP protocol, which all ISPs use by default, is to manage these hops, although failure to broadcast certain network segments can cause some routes to lengthen. BGP requires a full mesh of internal BGP sessions, which are connections between routers within the same autonomous system. To improve scalability, BGP route reflectors or confederations can be used.

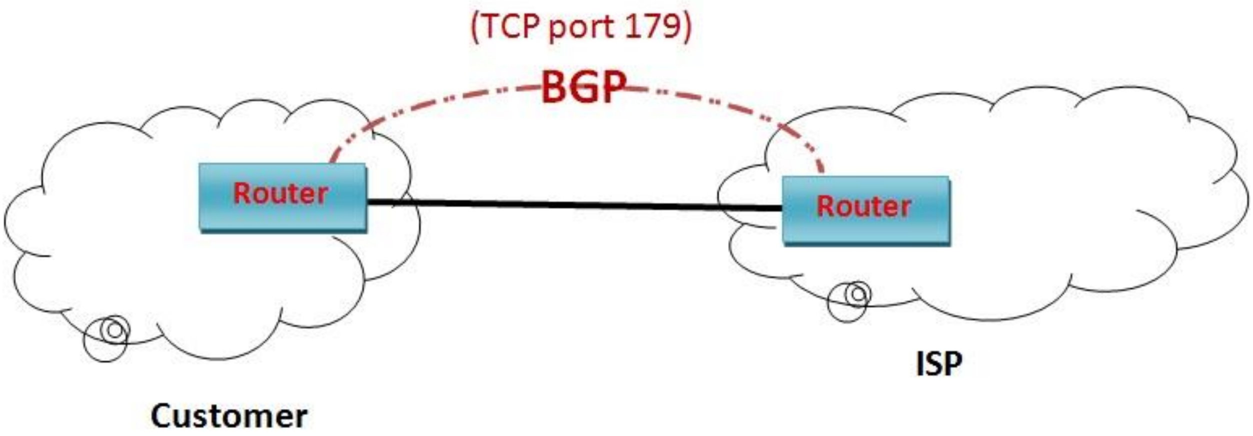


Figure 12 Approach

BGP uses TCP to establish a stable connection on port 179 between two BGP speakers, also known as neighbors or peers. Each BGP session involves creating exactly one TCP session between the peers. No routing information can be exchanged until this TCP session is established. This means that any BGP speaker must have an operational IP connection, usually provided through a direct physical link or an IGP.

Since BGP uses TCP, it doesn't need to handle transport issues like data sequencing or fragmentation; TCP manages these concerns and provides BGP with a reliable channel for its messages. For additional security, MD5 signatures can be used to authenticate each TCP segment.

3.2 Tools for BGP Management

3.2.1 Prefix Sanity Checker (PSC)

Purpose and Functionality: The Prefix Sanity Checker (PSC) is a tool designed to verify and format IP prefixes before they are broadcast over BGP. It ensures that IP prefixes are correctly formatted and meet the required standards for network configurations.

- **Key Features**:
    - Accepts IP address lists in various formats.
    - Generates IP prefixes compatible with Cisco and Juniper devices.
    - Flags incorrectly formatted prefixes and ensures they are rejected before broadcast.

Real-World Application: In the UK, ISPs such as BT and Virgin Media utilize PSC to maintain accuracy in BGP configurations. For example, PSC helps prevent errors like IP address overlaps or incorrect subnetting, which could otherwise lead to network disruptions or inefficient routing.

Technical Details: PSC employs regular expressions and validation algorithms to parse and validate IP prefixes. It cross-references these prefixes with established databases of valid address formats and prefixes, ensuring compliance with RFC standards.

3.2.2 Prefix Hijack Alert System (PHAS)

Purpose and Functionality: The Prefix Hijack Alert System (PHAS) monitors BGP routes to detect and alert network administrators about prefix hijacking events. This includes unauthorized ASes announcing prefixes they do not own or modifying routing information inappropriately.

- **Key Features**:
    - Real-time notifications when BGP origin AS changes.
    - Detection of suspicious activities, such as the advertisement of more specific prefixes.

Real-World Application: PHAS has been instrumental in detecting and mitigating prefix hijacking incidents. For example, in 2018, PHAS helped a UK ISP identify and address a hijacking attempt by a smaller AS, enabling quick remediation and reducing impact on end-users.

Technical Details: PHAS continuously monitors BGP updates, using pattern-matching and anomaly detection techniques. It compares current BGP announcements with historical records to identify unusual changes, providing timely alerts to network administrators.

3.2.3 BGPStream

Purpose and Functionality: BGPStream is an open-source platform for analyzing BGP data, both in real-time and from archived sources. It facilitates the monitoring of routing trends and the diagnosis of network issues.

- Key Features:
  - Collects BGP data from various sources.
  - Uses Python’s pickle for data serialization and matplotlib for visualization.

Real-World Application: In the UK, BGPStream is used by network operators to analyze routing trends and detect anomalies. For example, during the 2020 BGP route leak incident, BGPStream was used to trace the source and spread of incorrect routing information, aiding in rapid issue resolution.

Technical Details: BGPStream gathers BGP data through a C-based API, processing and analyzing it using Python bindings. The tool's visualization capabilities help in interpreting complex routing data, making it easier to identify and address network issues.

3.3 Integration of Tools into Research Methodology

To effectively manage BGP routing and ensure network integrity, the following methodology integrates the PSC, PHAS, and BGPStream tools:

1. **Prefix Verification**:

   - Process: Utilize PSC to validate IP prefixes before they are broadcasted over BGP.
   - Objective: Ensure all prefixes conform to correct formats and standards, minimizing configuration errors.

2. **Monitoring and Alerting**:

   - Process: Deploy PHAS to monitor BGP routes and detect prefix hijacking or suspicious changes.
   - Objective: Provide real-time alerts for prefix hijacking incidents, allowing prompt response to security threats.

3. **Data Collection and Analysis**:
   - Process: Use BGPStream to collect and analyze BGP data, integrating results from PSC and PHAS.
   - Objective: Monitor routing performance, identify trends, and diagnose issues based on combined data from prefix verification and hijacking alerts.

Integration Flowchart:

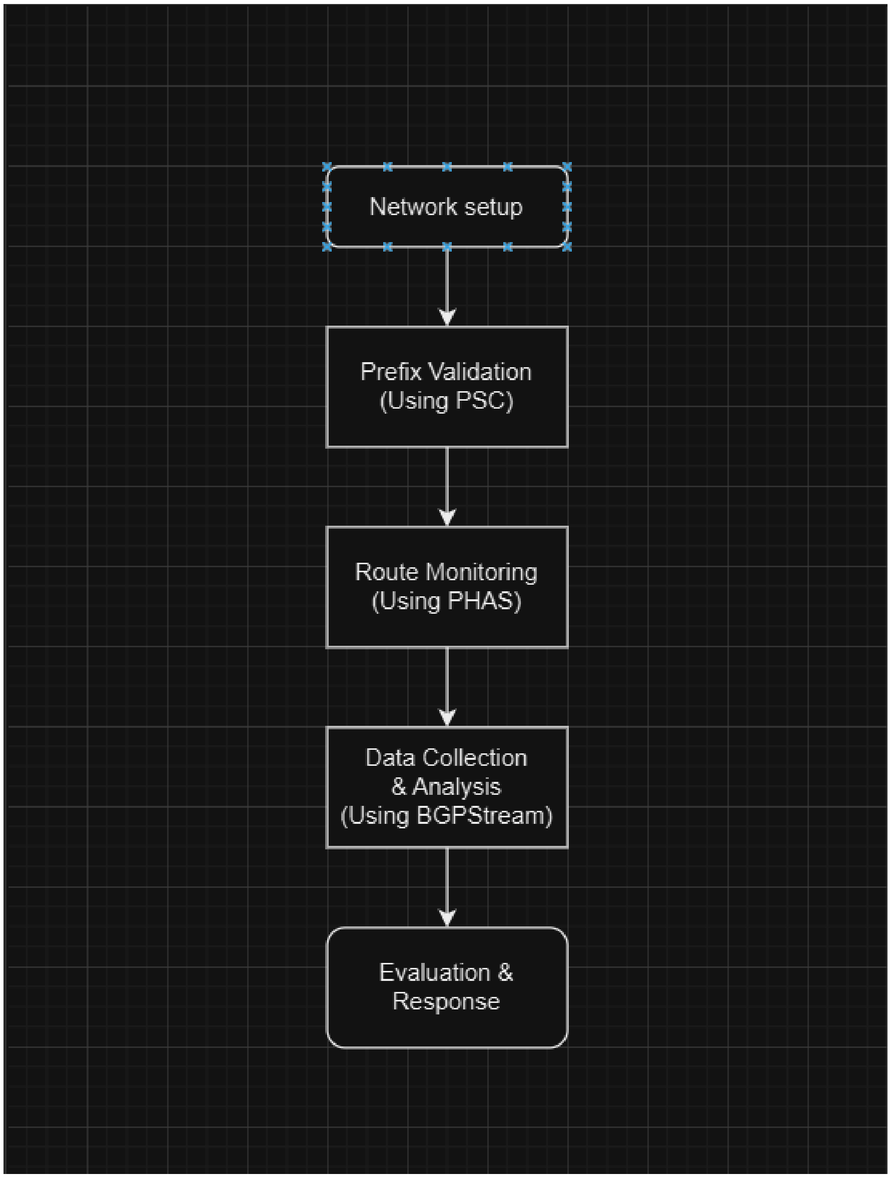

Network setup
Prefix Validation (Using PSC)
Route Monitoring (Using PHAS)
Data Collection & Analysis (Using BGPStream)
Evaluation & Response

Figure 13 Integration Flowchart (diagrams, n.d.)

In this integrated approach, PSC ensures prefix validity, PHAS provides real-time monitoring and alerting, and BGPStream offers comprehensive data analysis. This methodology enhances network performance, security, and operational efficiency.

Chapter 4

4 BGP SCALING

4.1 BGP Route Refresh

The BGP Enhanced Route Refresh feature is designed to help BGP neighbors detect and correct any discrepancies in their routing information. This functionality is activated by default and includes two optional timers to manage the process effectively.

Detailed Explanation:

Session Setup: When BGP neighbors establish a session, they exchange information about their capability to use the Enhanced Route Refresh feature. This feature is typically enabled by default, ensuring that most BGP sessions benefit from its capabilities.

Route Synchronization: Although it is uncommon for BGP neighbors to become inconsistent with each other, the Enhanced Route Refresh feature plays a crucial role in identifying and resolving such issues if they arise. This ensures that the routing information remains accurate and up-to-date.

Operational Process:

- Start-of-RIB (SOR) Message: When both BGP neighbors support Enhanced Route Refresh, each neighbor sends a Start-of-RIB (SOR) message before advertising its routing information (known as Adj-RIB-Out). This marks the beginning of the route advertisement process.
- End-of-RIB (EOR) Message: After advertising the routes, an End-of-RIB (EOR) message is sent. This message signifies the completion of the route advertisement process.
- Route Refresh Reply: Upon receiving an EOR message from a neighbor, a BGP speaker will remove any routes that were not included in the neighbor's Route Refresh reply. This helps ensure that the routing tables remain synchronized and accurate.

Ensuring Route Consistency:

- Expired Routes: If a router still has expired routes after receiving the EOR message or after the EOR timer expires, it indicates that there were inconsistencies between the neighbors. This situation is used to determine whether the routing information is consistent.
- Identifying Issues: The Enhanced Route Refresh feature helps identify and correct these inconsistencies without requiring a hard reset of the BGP session, which can be disruptive.

By leveraging the BGP Enhanced Route Refresh functionality, network administrators can maintain accurate and consistent routing information across BGP neighbors. This feature minimizes disruptions and ensures that routing tables are synchronized, improving the overall stability and performance of the network.

BGP Enhanced Route Refresh Timers:

Under normal circumstances, you don't need to configure these timers. However, if you experience persistent route flapping, causing difficulties in generating a Route Refresh EOR message, you may need to set one or both of the timers. Here's a detailed explanation of each timer and their functions:

4.1.1 Timers and Their Functions:

Stale Path Timer:

- Purpose: The Stale Path Timer is used when a router should receive an EOR message but does not.
- Function: When the bgp refresh stalepath-time command is set, the router starts this timer upon receiving a Route-Refresh SOR message. If the router does not receive a Route-Refresh EOR message after sending its Adj-RIB-Out, the stale routes are removed from the BGP database once the timer expires.

Maximum EOR Timer:

- Purpose: The Maximum EOR Timer is used when the router is unable to generate an EOR message.
- Function: When the bgp refresh max-eor-time command is set, the timer starts if the router cannot create a Route-Refresh EOR message. When the timer ends, the router forces the generation of a Route-Refresh EOR message.

Customization and Defaults:

- Both timers are customizable to suit specific network needs.
- By default, both timers are disabled and set to 0 seconds.
- If these timers are not configured, the router will remove stale routes from the BGP table if no Route-Refresh EOR message is received within 800 seconds.
- Similarly, if no Route-Refresh EOR message is generated within 800 seconds, the router will create one.

4.1.2 Practical Usage:

Stale Path Timer:

- This timer helps ensure that outdated routes do not remain in the BGP table for too long if there is a failure in receiving an EOR message.
- It starts when a Route-Refresh SOR message is received and runs until an EOR message is expected. If the EOR message is not received within the set time, the router clears the stale routes.

Maximum EOR Timer:

This timer ensures that an EOR message is generated even if the router initially fails to create one.

It starts when there is a need to generate an EOR message. If the router cannot generate the message within the specified time, the timer ends, and the router forces the creation of the EOR message. By configuring these timers, you can manage and mitigate issues related to route flapping and ensure that your BGP routes remain consistent and up to date.

4.2 BGP Confederation

Network engineers can use BGP confederations to manage the complexity and size of large autonomous systems. BGP confederations can be an alternative to BGP route reflectors or can be used alongside them. The concept behind BGP confederation is to divide an autonomous system (AS) into smaller, more manageable sub-autonomous systems (sub-ASs), each with its own AS number. This approach provides a scalable solution for BGP deployment and management within a large AS.

Implementing BGP confederation reduces the overall number of BGP connections within an AS and the number of iBGP peering sessions per router. A high number of iBGP sessions can consume significant resources and create excessive CPU load, negatively impacting throughput. To address iBGP scalability challenges, network engineers can use either BGP confederations, BGP route reflectors, or both.

BGP route reflectors, unlike confederations, do not require major changes to the existing setup and topology. Instead, certain routers are designated as focal points for iBGP sessions within a single AS, each using its own IGP. This method simplifies the iBGP session management without altering the underlying network architecture significantly.

Deploying BGP confederations involves substantial changes to BGP settings and the overall network architecture, adding complexity to achieve a reliable and scalable BGP network. However, the key advantage of a confederation is its ability to support various IGPs within different sub-ASs, providing greater flexibility for network expansion. Consequently, choosing a confederation over route reflectors is more appropriate when the IGP reaches its scalability limits and becomes difficult to manage, especially if there is a need to handle multiple independent ASs, each potentially using a different IGP.

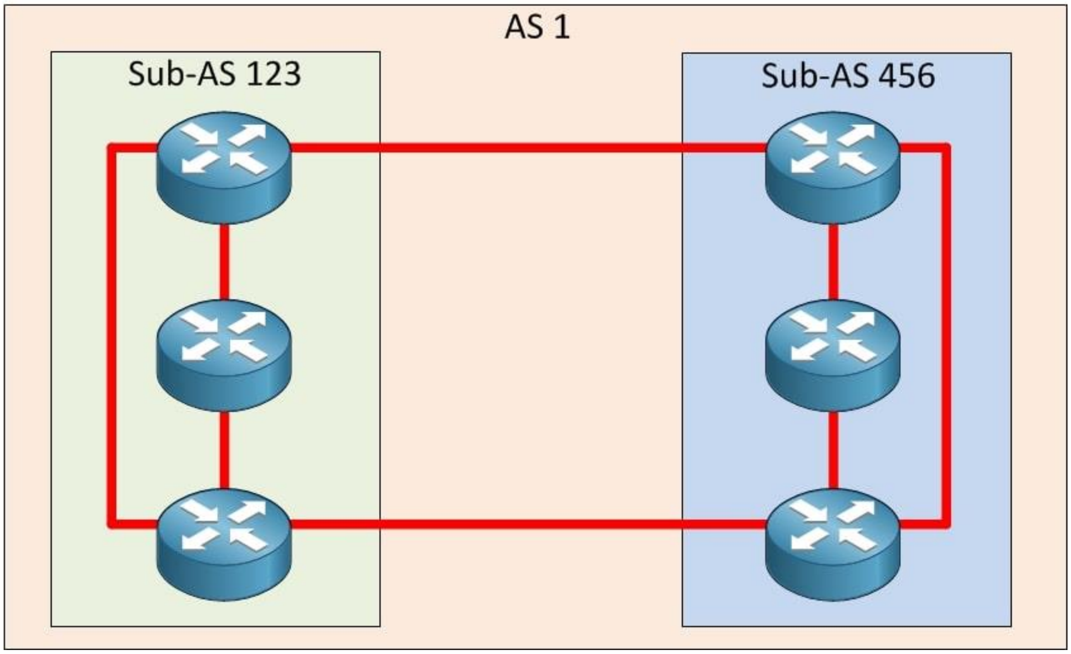


Figure 14 BGP Confederation

The image above illustrates the concept of dividing a single autonomous system (AS) into multiple sub-autonomous systems (sub-ASs). Each sub-AS operates with its own unique AS number and adheres to its own internal BGP (iBGP) rules, potentially running a different interior gateway protocol (IGP) than other sub-ASs within the confederation.

Within each sub-AS, all BGP speakers are fully meshed, enabling them to learn external routes and exchange external routing information effectively.

Path Selection and Routing Preferences:

When BGP needs to select the best path to a destination, it considers various factors based on the type of routes available. Routes exchanged between sub-ASs, known as confederation external routes, are prioritized over iBGP routes within the same sub-AS. If BGP must choose between two paths to the same destination—one within the sub-AS and another outside the sub-AS but still within the confederation—it will prefer the external path leading to the adjacent sub-AS.

However, when deciding between a confederation eBGP route (within the confederation) and an eBGP route that leads beyond the confederation, BGP will always prefer the external route beyond the confederation. This preference ensures that routes to destinations outside the confederation are prioritized, helping to maintain efficient routing.

Loop Avoidance and AS Path Attribute:

An eBGP connection between sub-ASs also serves as a loop-avoidance mechanism. The AS path list shared between eBGP neighbours within a confederation is crucial for this purpose. If a routing update leaves one sub-AS and attempts to return to the same sub-AS, the AS path list is checked. If the update detects its own sub-AS number in the AS path list, it will reject the update, thereby preventing routing loops.

The **AS_PATH Attribute** is an essential characteristic in BGP. It records the sequence of autonomous system numbers that a route has traversed on its way to its final destination, including the AS number from which the route originated. Each time a routing update passes through an AS, that AS's number is added to the list. Notably, the AS_PATH attribute in a routing update is only modified when the update crosses an eBGP boundary. This attribute plays a crucial role in both loop prevention and determining the most efficient route.

There are two standard parameters of AS_PATH attribute-

- AS_SET: an unsorted collection of ASs which a route has passed through
- AS_SEQUENCE: the ordered list of ASs which a route has passed through
- AS_CONFED_SET: an unsorted list of sub-ASs which a route has passed through in confederation
- AS_CONFED_SEQUENCE: In confederation, an ordered collection of sub-ASs which a route has traveled.

Only routers that advertise routes to their eBGP neighbors are assigned the AS number. This means that if a router sends a route update to another sub-AS, it does so in an eBGP session within the group and adds its own sub-AS number to the list. There are additional things to keep in mind when looking at eBGP in a cluster. When all subnets in a subnet use the same IGP, properties such as next hop, MED, and local preferences may not change when routing updates are transmitted across the link. eBGP, unlike regular eBGP. When eBGP is deployed in a group, it works the same as iBGP.

4.3 BGP Messages

Four message kinds are used in BGP connectivity. With the TCP connection, all BGP messages are unicast to a single peer.
BGP message types-

- OPEN –
  Open messages initiate a BGP connection by requesting that a BGP session be established across an ongoing TCP/IP connection. When both BGP routers finish a TCP 3-way handshake, they would begin to create a BGP session through Open messages. Before establishing a BGP peering, both entities exchange session capabilities. The BGP version, ASN of an originator router, Hold Time, BGP Identifier, as well as other optional elements which create session capabilities are all included in the OPEN message.

- KEEPALIVE –
  BGP may not depend on a TCP connection state to determine whether or not peers still are active. Keepalive messages are sent every one-third of a Hold Timer set by both the BGP routers. If a router acknowledges the Open message's payload, it replies with Keepalive.

- UPDATE –
  The Update message might promote any viable routes, remove existing advertised routes, or both. While advertising prefixes, the Update message contains Network Layer Reachability Information (NLRI), which provides the prefix and related BGP PAs.

- NOTIFICATION –
  This message is issued if something terrible occurs, such as an issue that forces the BGP session to terminate. (ciscopress, n.d.)

4.4 BGP Route Reflector

Redundant Reflection (RR) is a way to rid an entire network of IBGP traps. The router informs all IBGP routers across the network of available routes without creating loops. The purpose of RR is key, that is, instead of looking at every router in the whole mesh, multiple BGP routers can look at the same point, **RR**, which acts as a router mirror provider. (networklessons, n.d.)

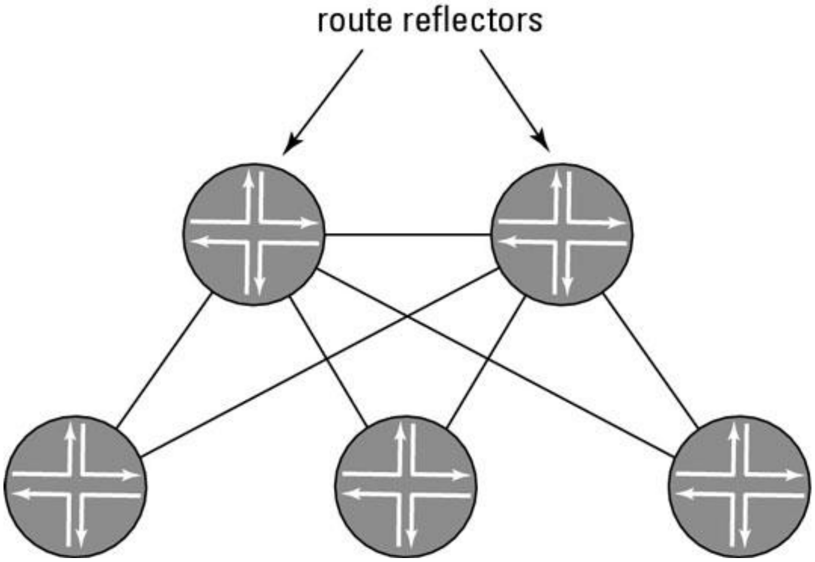


Figure 15 Route Reflector

Every other IBGP router becomes a route reflector client. The idea of route reflection allows one or more routers to be designated as route reflectors.

4.4.1 eBGP Neighbors

Before exchanging routing information, BGP, like OSPF or EIGRP, establishes connections with other BGP routers. In contrast to certain other routing protocols, BGP doesn't really employ broadcast or multicast to "find" additional BGP neighbors. Neighbors that BGP will connect to via TCP port 179 must be specified.

The local router's ASN (as specified by the bgp asn router command) must match the router's reference to that ASN as specified by remote neighbor-asn Command The BGP router IDs of the relevant routers cannot match.

4.4.2 BGP Client Neighbor

A link from a client’s peer across all non-client peers and client peers can be termed as BGP Client neighbor. Here, full mesh topology is not required. The other clients and route reflectors form a cluster.

4.4.3 BGP Non-Client Neighbor

A route from a non-client iBGP peer is advertised to all clients. Fully meshed topology is required. The non-client neighbors sit outside of the cluster which is formed by the clients. The non-client is simply another iBGP peer to the route reflector. As a result, the route reflector may follow the BGP split-horizon rule, which means that routes from non-clients are only reflected to clients.

Chapter 5

5 Implementation

5.1 implementation

When BGP is running. The first step is to enable BGP routing. BGP must be able to obtain the router's address (eg, a configured loopback address). In the BGP router configuration, the communication group must be defined individually, but the communication group must also be defined in the peer. BGP determines if multiple peers are connected by establishing eBGP neighbor ships. By default, BGP does not attempt to establish connections between peers that are not directly connected.

If multiple BGP neighbors are not physically linked and peering among the routers loopbacks is necessary, we can use “ignore-connected-check command”. The above command bypasses BGP's normal inspection, which can see if the source IP in BGP control packets is on the same network as the destination. A TTL of 1 is sufficient if an ignore flag is used. Configuration changes made to a specific BGP instance can be done simultaneously. On the other hand, it is not possible to change or improve for different events at the same time.

Each AS is highly interconnected within itself, with few connections to other independent systems in the same group. This group follows other key concepts that allow you to use an Internal Gateway Protocol (IGP) with all AS devices. (cisco, n.d.)

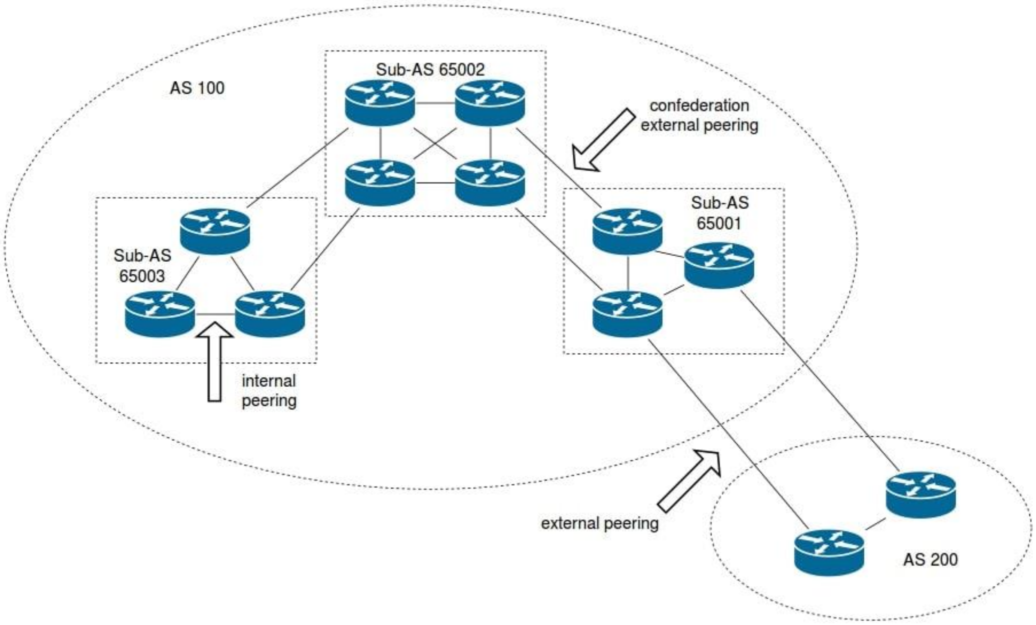


Figure 16 Confederation and set of sub-AS

BGP route reflectors and BGP confederations are two tools that can help user maintain the amount of sessions under control, with route reflectors of been the most frequently used. As we know that Confederation is the division of an AS among set of sub AS, it is essential to remember this that external confederation BGP is not same as eBGP. It has the same loop avoidance technique as eBGP, and so by depending on the eBGP-sequel method, we no more need to maintain a decent iBGP network over the whole BGP. (techtarget, n.d.)

The BGP route reflector criteria are straightforward:

- Anything and everything that a route-reflector client or an external BGP peer sends would be transmitted to every neighbor.

- Whatever information is received from a router that is not a route-reflector client is solely transmitted to clients and external BGP neighbors.

With these two settings in mind, we can traverse the BGP session graph in our network, inspecting each BGP router along the way to make sure they haven't violated the route reflector requirements. BGP prefixes are directed on each router to all other routers that use these rules.

Another typical reason that an IP prefix is not broadcast throughout the network is that external subnets at the edges of the network are not published to the core routers.

Whenever an IP prefix is issued to such an internal BGP neighbor, the next router's IP address remains unchanged. The IP address of a router that is one hop across the boundary of an autonomous system is often the IP address of the next hop of an external route. The IP subnets that connect the edge routers to their respective external neighbors must be integrated with the internal routing system, such as OSPF or IS-IS. Otherwise, an internal BGP router will determine that the BGP next hop is unreachable and ignore the IP prefix. This will be included in the BGP table, but will not be used or forwarded to other BGP neighbors.

Although all core routers in the network may be running BGP, internal BGP sessions do not need to adhere to the physical fabric of the network. For example, some core routers can serve as route reflectors for all BGP routers in the network.

5.2 Flow-tag propagation

Using the flow-tag propagating function, we may build a relationship between route-policies and user-policies. BGP flow label propagation helps visitor traffic to route based on network parameters such as AS number, prefix entry, community values, including extended communities. Outbound ads influence inbound traffic, while inbound ads influence outbound traffic.

Flow-tag propagation is used for:

- Classifying communications depending upon target IP addresses and perhaps even prefixes.
- Choosing a TE-group which corresponds to such cost of any route towards the provider.
- Implementing traffic policies for individual consumers.
- Diverting the traffic which should be sent to a software or caching servers.

Chapter 6

Network Test

For testing the BGP connectivity, there are some points and measure we should take care of, which further I have mentioned in this particular topic. Let us see how can we confirm the connectivity and make sure that there are no issues.

6.1 Detailed Verification Process for BGP Neighborship

Verifying BGP neighborship is crucial to ensure that routing information is being accurately exchanged between routers. The verification process differs depending on the type of router—whether it's an internal router, a border router, or an advertised BGP router. Here, we outline specific commands for each router type and the key indicators to look for in their outputs. (cisco, n.d.)

6.1.1 Internal Routers

Internal routers manage BGP sessions within an autonomous system. Ensuring these sessions are properly established is vital for internal network stability.

- **Commands to Run:**
  - **show ip bgp summary**: This command gives an overview of all BGP sessions, displaying the status, uptime, and number of prefixes received. Look for all sessions to be in the "Established" state.
  - **show ip bgp neighbors:** Provides detailed information about each BGP neighbor, including the Autonomous System (AS) number, BGP version, and message statistics. Verify that the AS numbers match expected neighbors and that no unexpected neighbors are listed.

6.1.2 Border Routers

Border routers handle the traffic exchange between different autonomous systems. Ensuring these routers are correctly configured is essential for maintaining external network connections.

- **Commands to Run:**
  - **show ip bgp neighbors:** Offers comprehensive details about each BGP peer, including the state of the connection and the routes being received. Verify that all external neighbors are correctly established and that no errors are reported.
  - **show ip bgp paths:** Displays detailed routing paths, which helps confirm that the routing information exchanged with external peers is accurate. Look for discrepancies between expected and actual routing paths.

6.1.3 Advertised BGP Routers

Advertised BGP routers are responsible for sharing routes with external networks. Ensuring these routes are correctly advertised is crucial for network reachability.

- **Commands to Run:**
  - **show ip bgp neighbors <neighbor_ip> advertised-routes:** This command checks the specific routes being advertised to a neighbor. Ensure that the advertised routes align with the network's routing policies.
  - **show ip route:** Confirms that the advertised routes are present in the routing table and are being propagated as expected.

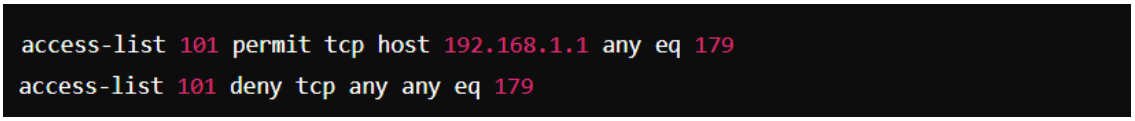
6.2 Securing BGP Against TCP-Based Attacks

BGP relies on TCP for establishing sessions between routers, making it vulnerable to various TCP-based attacks such as session hijacking, spoofing, and denial-of-service (DoS) attacks. Implementing robust security measures is critical to protecting BGP sessions.

6.2.1 Access Control Lists (ACLs)

Access Control Lists (ACLs) are a primary defense mechanism for securing BGP sessions. ACLs can be configured to limit which IP addresses are allowed to establish BGP sessions on TCP port 179, reducing the risk of unauthorized access.

- **Example ACL Configuration:**



```
access-list 101 permit tcp host 192.168.1.1 any eq 179
access-list 101 deny tcp any any eq 179
```

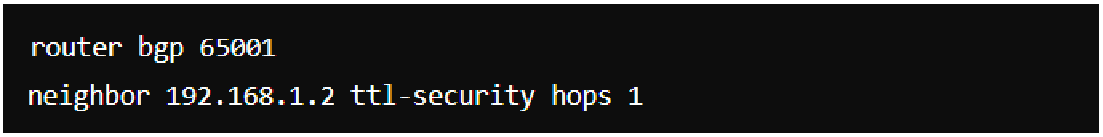
Figure 17 ACL Configuration (Arduino)

This configuration ensures that only the IP address 192.168.1.1 can establish a BGP session on port 179, blocking unauthorized attempts to access the session.

6.2.2 Generalized TTL Security Mechanism (GTSM)

The Generalized TTL Security Mechanism (GTSM) is an effective way to protect BGP sessions from spoofed attacks. GTSM limits the number of hops a BGP packet can take, ensuring that packets from non-directly connected devices are discarded.

- **Configuring GTSM:**



```
router bgp 65001
neighbor 192.168.1.2 ttl-security hops 1
```

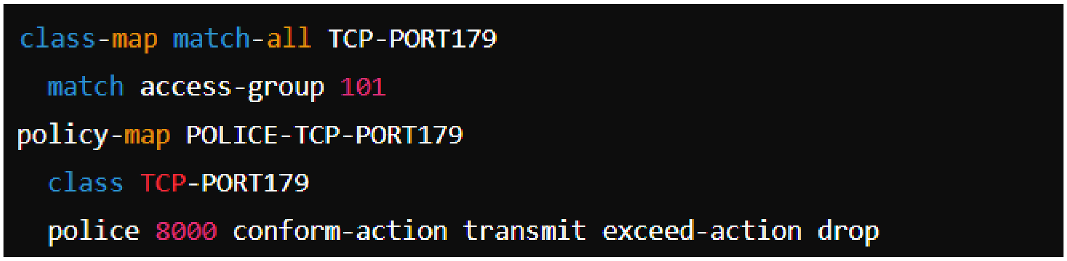
Figure 18 Configuring GTSM

This configuration secures the BGP session by setting a TTL value that limits the session to directly connected devices, thus preventing spoofed sessions.

6.2.3. Mitigating TCP Resource Exhaustion

TCP Resource Exhaustion attacks target BGP's reliance on TCP port 179 by overwhelming the router with connection requests. To mitigate this, rate-limiting incoming TCP connections and using features like SYN cookies can prevent such attacks from disrupting the network.

- **Rate-Limiting Example:**



```
class-map match-all TCP-PORT179
  match access-group 101
policy-map POLICE-TCP-PORT179
  class TCP-PORT179
  police 8000 conform-action transmit exceed-action drop
```

Figure 19 Rate-Limiting Example (Python)

This configuration rate-limits the incoming TCP packets targeting port 179, ensuring that the router is not overwhelmed by malicious traffic.

In the next chapter we will see the optimization techniques of BGP.

Chapter 7

BGP Optimization

With the spread of the Internet in our daily lives, users are looking more and more to be able to access it seamlessly, anywhere, anytime and without interruption. It is now possible to move a single IP device from one Internet access point to another without losing higher-level connections. To improve the reliability and speed of the Internet, the efficiency and functionality of the routing protocol that allows the Internet to function must be improved.

The routing protocol defines how routers communicate with each other. A router first sends routing information to its local network neighbors, then to the rest of the network. The path followed by the routers creates the network topology. Border Gateway Protocol (BGP) is a universal external gateway routing protocol that communicates routing information between independent computers on the Internet backbone.

7.1 BGP Vulnerabilities

Since BGP is built on integrity by design, there is a vulnerability. BGP routers determine the shortest and most efficient path for data to reach the destination so that different ASs can interact. BGP, on the other hand, believes that if a router advertises the optimal route, it is telling the truth. It is necessary to examine a risk paradigm in addition to obtaining a precise view and understanding of BGP vulnerabilities. The paradigm should be able to provide an overview of all the many types of attacks that determine the capabilities of attackers to target the network. The overview should include a description of the attacks, the malicious elements involved, the effects of the attack, the purpose of the attacks and a complete documentation of the results. (network insight, n.d.)

BGP is a global protocol implemented by tens of thousands of routers. Therefore, there are many cases where an attacker can launch an attack. Each autonomous system interfaces with other ASs over the Internet in an informal manner. Using such size and interconnection, adversaries can influence routers and networks far from their respective neighbors.

The results of such cyber-attacks are as varied as their methods. An attack can lead to unexpected termination of BGP connections, network and AS inaccessibility, fragmentation of the address field, as well as many undesirable effects. Threats can be used sequentially to increase their impact or trigger more hostile actions. A particular router can be taken down with data, taken over or controlled by an intruder. Information from an autonomous system may be blocked or redirected in some way, and transmissions to or from it may be significantly impeded or dropped altogether. Faulty ASs force their neighbors to calculate links or modify the existing forwarding table.

Route Flapping

Whenever a route is offered and then withdrawn frequently, it usually referred to as 'flapping.' This is not the same as type route oscillation. Oscillation occurs on a regular basis, although flaps may not Route flaps are the most significant source of insecurity across the Internet and within any network. It happens when a legitimate route is considered illegitimate and subsequently repealed. The difficulty is obvious because it leads the router to continually alter existing status, and even the update is broadcast across the internetwork, forcing the router to perform necessary synchronizations.

Humans are one other major root for route flaps, probably the most notable of all; specialists fiddling inside the Telco call center or the wire vault may undoubtedly create breakdowns that result to flaps. However, unskilled network operators can often drop a route, change the state of an interface, or clean up a BGP connection while adjusting or debugging a router, or an attack can trigger the damping of a victim's route.

The router is unable to process the modifications and crashes. Downstream routers must therefore handle not just the initial flapping routes, but as well every routes that have become inaccessible as a result of the failing router. The consequences can cascade all across network, perhaps leading many routers to malfunction. (catchpoint, n.d.)

7.2 Cryptographically enhanced BGP

Cryptography is perhaps the foremost commonly used technique in BGP protection study. The goal has been to give authentication information in addition to the capacity to safeguard data from eavesdropping by employing encryption and secure digital signatures. For instance, where was the data originate from, plus who permitted it?

To safeguard BGP, cryptography may be used at several levels, namely connection, route update, and route table.

Address block, Autonomous Number, Path data (attributes), Original address blocks (allocated according to IANA/RIR), trusting the peers/neighbors are the main components to be taken care of.

Cryptographic Hash Functions

Cryptographic hash functions, generally defined as digest algorithms, generate a resolved hash result from source information and serve as the foundation for message authentication code as well as digital signatures. The MessageDigest algorithm 5 (MD5) and also the Strong Hash Algorithm group, notably SHA-1, are most often used hash functions today. Take into account an effort to obtain a message which will link to a specific MD5 digest with a 128-bit digest. This would take an estimate of 2127 texts to identify the specific message which linked to a digest value, or 264 messages to obtain a message that formed a collapse, a distinct message that plots to the very same digest value.

Structural Safety

Attempts are now being made throughout standard organisations and research communities to create more complete BGP security designs. The design includes a set of security services as well as a detailed security analysis. Secure BGP (S-BGP) was developed as an addition to BGP by experts at BBN (Bolt, Beranek, and Newman) and became the initial to complete routing security solution aimed especially at BGP with the goal of protecting BGP against inaccurate or malignant UPDATES. Each data transferred via S-BGP is authenticated via PKI certificates, and AS statements are verified with the accompanying private key. The organization getting the verified data validates it by utilizing S-two BGP's important capabilities, Address Attestations (AA) & Route Attestations (RA). (ieeexplore, n.d.)

Address Attestations (AA):

Address Attestations is securely authenticated assertions issued by prefix's originator and then used to validate prefix identity and published route. Address attestations assert the ability to create an prefix, sign it, and transmit it outside of band. An out mechanism doesn't really explicitly utilize a BGP system to convey data; rather, it communicates pertinent data through another connection or service.

Route Attestation (RA):

Route attestations typically transmitted inside S-BGP as more than just a new property in a customized BGP UPDATE message, enabling a nearby AS to broadcast the route included in that UPDATE. Each AS signs a route attestation as it travels the network, while all ASs upon on path verify earlier connected identities. When UPDATE messages are sent among neighbors, the recipient neighbor verifies that information prior transmitting it on to other peer. As a consequence, a ‘‘onion-style" verification with identities from across all routers along the route is produced.

Nevertheless, although S-BGP offers the most extensive security assurances of any approach by giving complete verification of sources as well as routes to recipients, it faces substantial hurdles to implementation. Moreover, one implementation impediment was because it necessitates the availability of a layered PKI infrastructure and transmission system which is acknowledged by other involved ISPs.

Difficulties in S-BGP:

- S-BGP is somewhat cryptographically demanding, necessitating every UPDATE to have validated and acknowledged from each S-BGP router by which it goes. Because of the huge amount of routes which will get created in such a small time frame, this throughput overhead is unconscionable for initiating a BGP peering connection.

- Additionally, S-BGP cannot protect against collusion threats. These threats are feasible if multiple hacked routers pretend to have a straight connection among devices.

- The architectural challenge seems to be typically router requiring a considerable amount of storage for holding up all public keys for Route Attestations (RA).

- For a communicator having tens of peers, the space requirement could become enormous.

Public Key Architecture

The cryptography approaches rely on two entities sharing a shared key. Since notifications may come via any of the Web's over 35,000 ASs, it's indeed important to be capable to confirm the authenticity of such communications using techniques like as message authentication scripts and digital signatures, but also those depend mostly on creation of credentials (key) among AS neighbors.

Handling the Key’s globally, necessitates public key encryption. Within context of BGP, each AS seems to have a public key that is freely distributed to every single AS on the

Network, and even a private key that is rarely disclosed. If several ASs have no previous understanding of one another, then can establish a key for encrypted transmission unless they may locate that public key for such AS with which they desire to connect. The public key architecture, or PKI, offers a structure for the allocation and distribution of public keys.

TTL Mechanisms in general

The General TTL Security Mechanism, formerly known as the BBGP TTL Security Hack, describes a procedure to safeguarding peers versus remote threats. In an IP packet, the TTL property gets assigned to the figure which is decremented at each hop. IOS transmits BGP packets to peers with just a TTL of 1 by default, which implies that the peer stay immediately linked else the packets would expire during transmission.

Unfortunately, here is a drawback within that methodology: it's indeed easy for hackers to modify the TTL of transmitted packets to look as if they are coming from even a locally linked peer.

Secure Origin BGP

This is a technique to verify the accuracy as well as legitimacy of traffic transferred inside BGP, and also to mitigate cyberattacks caused by configuration errors or purposeful placement of incorrect traffic through the routing systems. All security-related details are communicated among neighbors through a SECURITY signal, a new message category in BGP provided by Secure Origin BGP.

Its purpose is to enable two data transmission components. First, it checks if an AS is authorized to generate a given prefix. Second, it ensures that an AS forwarding a prefix has at least one legitimate route to the endpoint. The secure origin protocol BGP focuses on the use of three types of certificates. The entity certificate is required to authenticate an AS, including the public key. The entity certificate associates an AS number, a component of the routing network, with the public key associated with that AS. Issuing organizations that allow the use of AS numbers and parts of the address space are not actually required to verify an entity's public key, and institutions that validate the organization's public key do not should be more necessary for legitimate advertising structures. rather, a third party must be sought.

As a result, the entity certificate is a distinct certificate type which validates who the entity is under the routing.

7.3 Temporal Cache Management Schemes

When an earlier confirmed correct update is re-announced with the similar unexpired (non-revoked) **SKIs (Subject Key Identifier)** as the initial version, the re-announced update does not require to be checked; in addition, the re-announced update could be ignored. There is no potential threat as a result of it.

While coping with timed updated channel circumstances, it's indeed important to examine that the optimization algorithms cached the existing validated update sections through time. Keeping this in mind, the subsequent methods are derived using these methods:

- **Cache Common Segments with RIB Cache (CCS-RC)**: Similar segments signature verification information are stored during RIB startup as well as from all ongoing trace queries inside this RIB-in. The cache records matching to retracted notifications (explicit or implicit) really aren't kept.

- **Cache Common Segments with Extended Cache (CCS-EC)**: This technique is an expansion of CCS-RC having the major improvement: all cache entries of all withdrew updates (explicit or implicit) get kept and transferred under an Extended Cache (EC). These cached identity confirmations inside the EC are seen in a similar manner as these in the RIB are.

- **Best Path Only with RIB Cache (BPO-RC):** The inclusion of caching the identical segments signature recognition findings for the chosen (current) best routes in a RIB cache. The caching records relating to every retracted statements (explicit or implicit) are just not kept.

- **Best Path Only with Extended Cache (BPO-EC)**: This method is an improvement to BPO-RC except that the cache entries of the verification outcomes relating to every retracted changes which were optimal routes be kept and transferred into such an Extended Cache (EC). These cached signature verifications throughout the EC are seen in the identical way as ones on the RIB do.

There is a lot of focus in network mobility in today’s date. Hence, optimizing the routes becomes an important factor to achieve the same. And as BGP is based on the Internet as the exterior routing protocol, which allows AS to interchange their routing information. Here, in the routing table modifications related to cache can lower the frequency of binding refreshes by a significant amount.

Chapter 8

Conclusion

To deal with route optimization, many techniques have indeed been offered. The great number of such protocols necessitate the implementation of new network elements or functions beyond the mobile network area. It clearly makes its implementation in the current Internet difficult.

The evolution of the volume of ASes employing BGP communities for data providers throughout time has indeed been significant.

The conclusion of the dissertation "Global Routing Optimization using BGP" highlights the essential role of the Border Gateway Protocol (BGP) in ensuring the stability and efficiency of internet routing. As the backbone of internet communications, BGP facilitates the exchange of routing information between different networks, known as autonomous systems (ASes). Its importance has only grown as the internet expands, necessitating ongoing improvements in both security and scalability.

One of the key advancements discussed is BGPsec, which enhances security by providing cryptographic validation for route announcements. This is crucial in preventing issues like route hijacking, which can disrupt internet connectivity. Additionally, the dissertation emphasizes the need for scalable solutions to manage the increasing data traffic and complexity brought about by technologies such as the Internet of Things (IoT) and 5G networks. These innovations rely heavily on robust routing mechanisms to handle a vast number of devices and the significant data they generate.

The research also addresses practical challenges organizations face when implementing BGP. For large tech companies like Google and Amazon, optimizing BGP is vital for maintaining high performance and security across their extensive networks. These companies must continually adapt their BGP strategies to balance efficiency with protection against potential threats.

Furthermore, the dissertation explores the integration of BGP management within broader organizational frameworks, particularly Project Portfolio Management (PPM). This approach is essential for aligning technical strategies with the overall goals of an organization. For example, non-profit organizations often operate under financial constraints and must ensure their network infrastructure is both reliable and cost-effective. Effective BGP management can lead to better resource allocation and improved outcomes in such contexts.

In summary, the dissertation concludes that ongoing research and development in BGP are crucial for meeting the future demands of the internet. By focusing on both technical enhancements and practical applications, the study aims to provide valuable insights for network administrators and organizational leaders. The findings underscore the necessity of a comprehensive understanding of BGP to navigate the challenges of a rapidly evolving digital landscape while ensuring a secure and efficient routing infrastructure for the global internet.

Bibliography

catchpoint, n.d. BGP Attributes. [Online]
Available at: https://www.catchpoint.com/bgp-monitoring/bgp-attributes
[Accessed 28 July 2023].

catchpoint, n.d. Vulnerabilities of BGP. [Online]
Available at: https://www.catchpoint.com/blog/bgp-vulnerabilities
[Accessed 20 July 2023].

cisco, n.d. Implement BGP. [Online]
Available at: https://www.cisco.com/c/en/us/td/docs/routers/ncs6000/software/ncs6k_r6-1/routing/configuration/guide/b-routing-cg-ncs6k-61x/b-routing-cg-ncs6k-61x_chapter_010.html#concept_pnb_vzb_mjb
[Accessed 23 July 2023].

cisco, n.d. Troubleshoot Common BGP Issues. [Online]
Available at: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/22166-bgp-trouble-main.html#anc5
[Accessed 17 July 2023].

ciscopress, n.d. BGP Fundamentals. [Online]
Available at: https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=3
[Accessed 5 August 2023].

cloudflare, n.d. What is BGP?. [Online]
Available at: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/
[Accessed 23 June 2023].

diagrams, n.d. Draw.io. [Online]
Available at: https://app.diagrams.net/
[Accessed 11 August 2023].

geeksforgeeks, n.d. Difference between EBGP and IBGP. [Online]
Available at: https://www.geeksforgeeks.org/difference-between-ebgp-and-ibgp/
[Accessed 9 August 2023].

ieeexplore, n.d. Security problems in BGP. [Online]
Available at: https://ieeexplore.ieee.org/document/6595458
[Accessed 17 July 2023].

inetdaemon, n.d. What is ASN. [Online]
Available at:
https://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/autonomous_system_number.shtml#:~:text=An%20Autonomous%20System%20Number%20(AS,homed%20to%20the%20public%20internet
[Accessed 9 July 2023].

network insight, n.d. Attacks on BGP. [Online]
Available at: https://network-insight.net/2014/12/attacking-border-gateway-protocol-bgp-at-the-internet-edge/
[Accessed 20 July 2023].

networklessons, n.d. BGP Attributes and Path Selection. [Online]
Available at: https://networklessons.com/bgp/bgp-attributes-and-path-selection
[Accessed 28 June 2023].

networklessons, n.d. BGP Communities Explained. [Online]
Available at: https://networklessons.com/bgp/bgp-communities-explained
[Accessed 17 July 2023].

networklessons, n.d. BGP Neighbor Adjacency States. [Online]
Available at: https://networklessons.com/bgp/bgp-neighbor-adjacency-states
[Accessed 7 August 2023].

networklessons, n.d. BGP Route Reflector. [Online]
Available at: https://networklessons.com/bgp/bgp-route-reflector
[Accessed 30 June 2023].
networklessons, n.d. Next Hop. [Online]
Available at: https://networklessons.com/bgp/bgp-attributes-and-path-selection#Shortest_IGP_path_to_BGP_next_hop
[Accessed 11 July 2023].
techtarget, n.d. How the routing protocol works. [Online]
Available at: https://www.techtarget.com/searchnetworking/feature/BGP-tutorial-The-routing-protocol-that-makes-the-Internet-work
[Accessed 11 July 2023].
techuk, n.d. Proximity expands UK footprint with Birmingham Edge Data Centre. [Online]
Available at: https://www.techuk.org/resource/proximity-expands-uk-footprint-with-birmingham-edge-data-centre.html
[Accessed 11 August 2023].
training.apnic, n.d. APNIC eLearning: BGP Attibutes. [Online]
Available at: https://training.apnic.net/wp-content/uploads/sites/2/2016/11/eROU04_BGP_Attributes.pdf
[Accessed 5 August 2023].

Summary

The University of West London
Faculty of Cybersecurity

Diploma Thesis Summary
Global Routing Optimization using BGP

Author: Jash Rajeshkumar Vaidya
Supervisor: Dr. Shidrokh Goudarzi

This Master's Dissertation is focused on the BGP routing protocol. Where, I have tried to discuss about the protocol from the basics. We need BGP routing optimization to enhance the network performance and stability mainly because today these are the main roots of a Network. Also.

With performance and Stability comes Security. Data being the most important factor brings Security and safety in frame and the main concern becomes integrity, because the network's integrity may be exploited, therefore all communication must be secured, and the trusted client must create a TCP connection to the IPStack by getting all of its traffic directed seamlessly inside the network.

Broken links, packet loss, long paths results in delayed responses, network failures or disconnections. These performance issues are the one's which we all have faced some or the other time. Reducing latency, shortening the routes can mainly benefit and also improve the variance if new routes are injected into BGP.