BGP Security & Attacks

By: Haseeb Ahmad, Talha Mahmood,
Artem Solovey, Yang Bai

What is it?

- **Border Gateway Protocol (BGP)** is a protocol that facilitates router-to-router communication and, as such, enables the exchange of routing-related information as well as discovery of optimal paths through the Internet.
- Or in simpler terms, BGP is the routing protocol of the Internet, used to **route** traffic across the Internet.
- Without it, we wouldn't even be able to do a Google search or send an email.

What is a **route**?

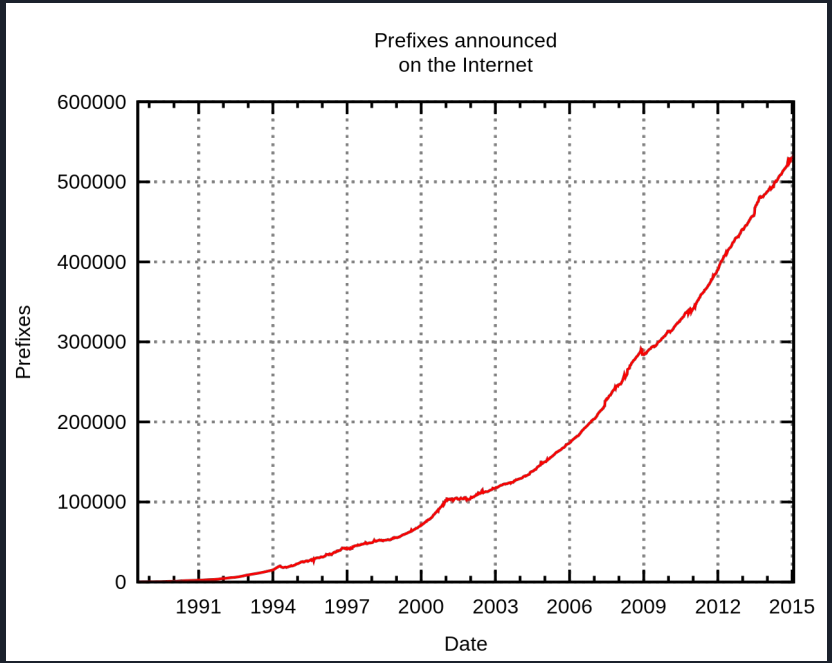
- *"The **name** of a resource indicates what we seek,*

  *an **address** indicates where it is,*

  *and a **route** tells us how to get there".*

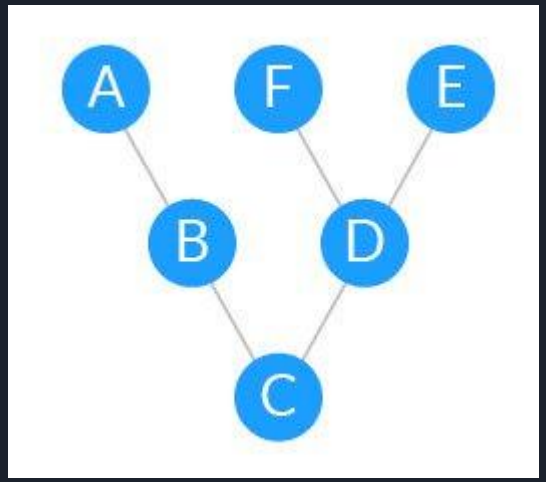
History

- In Internet's early days, there were only a few networks connected to each other. And because of this, routing between network nodes was quite static
- EGP (External Gateway Protocol) was invented to do the job.
- EGP is a simple routing protocol and is based on tree-like (i.e., hierarchical) topologies
- In modern networks, tree topologies were replaced by fully connected mesh topologies to allow for maximum scalability.

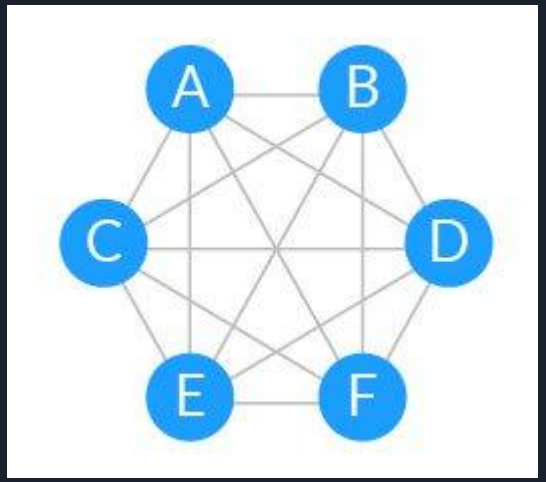


History

Tree-like vs. full mesh topologies



In a tree-like topology, to reach E or F, A will have to go through B, C and D.



In a full mesh topology, nodes have many paths to reach each other.

Autonomous System (AS)

- Can be an Internet Service Provider, a university or an entire corporate network.
- Each AS is represented by a unique number called an autonomous system number (ASN)
- Each autonomous system controls a collection of connected routing prefixes, representing a range of IP addresses.
- It then determines the routing policy inside the network.

The Internet
A Network of Networks

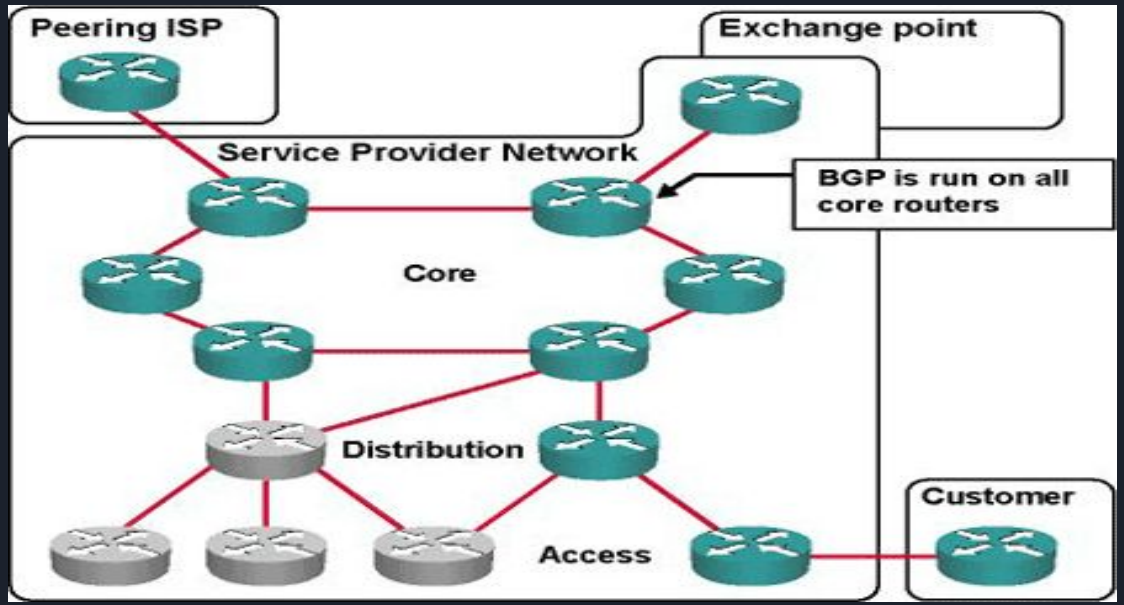
Who needs it?

- Network administrators of large organizations which connect to two or more ISPs
- Internet Service Providers (ISPs) who connect to other network providers

- **Not for:**
- Administrators of a small corporate network,
- or an end user

How BGP works

- BGP is always used as the routing protocol between ISPs but also as the core routing protocol within large ISP networks.
- It requires a full mesh of internal BGP sessions -- sessions between routers in the same AS.



BGP operation

- Each BGP speaker exchanges network reachability information with its BGP neighbours via BGP sessions
- BGP neighbors, called peers, are established by manual configuration between routers to create a TCP session on port 179
- Informations are stored in a router table named Routing Information Base
- Two types BGP sessions:
    1. iBGP - *internal*
    2. eBGP - *external*
- TCP is used as transport protocol for two BGP peers

BGP steps

1. Configuration between routers to create a TCP session on port 179
2. Once the TCP connection is established between the peers, OPEN messages are exchanged by which BGP speakers can negotiate optional capabilities of the session
3. Once the OPEN message is acknowledged by the peer router, UPDATE messages are used to exchange reachability information.
4. The other BGP messages include NOTIFICATION message which is sent by a router to indicate the ROUTE REFRESH message that is sent to request a retransmission of routing information.
5. A BGP speaker sends 19-byte KEEP-ALIVE message every 30 seconds to maintain the connection

BGP Message

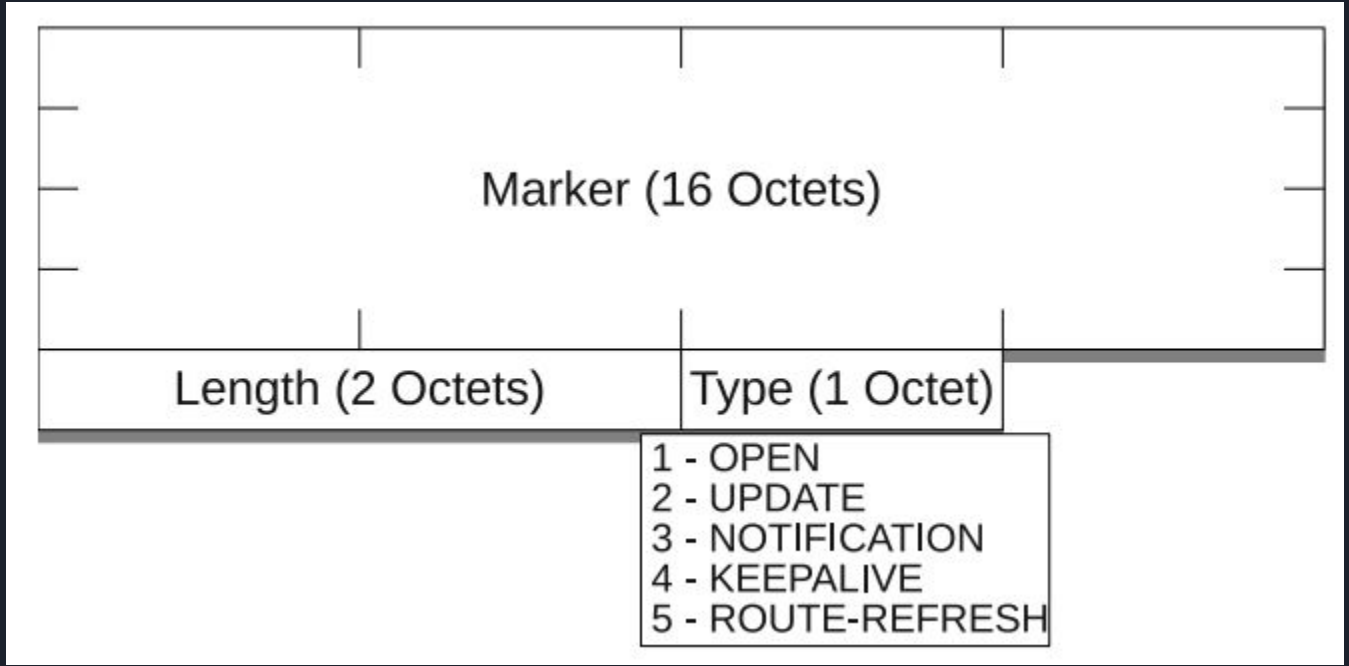
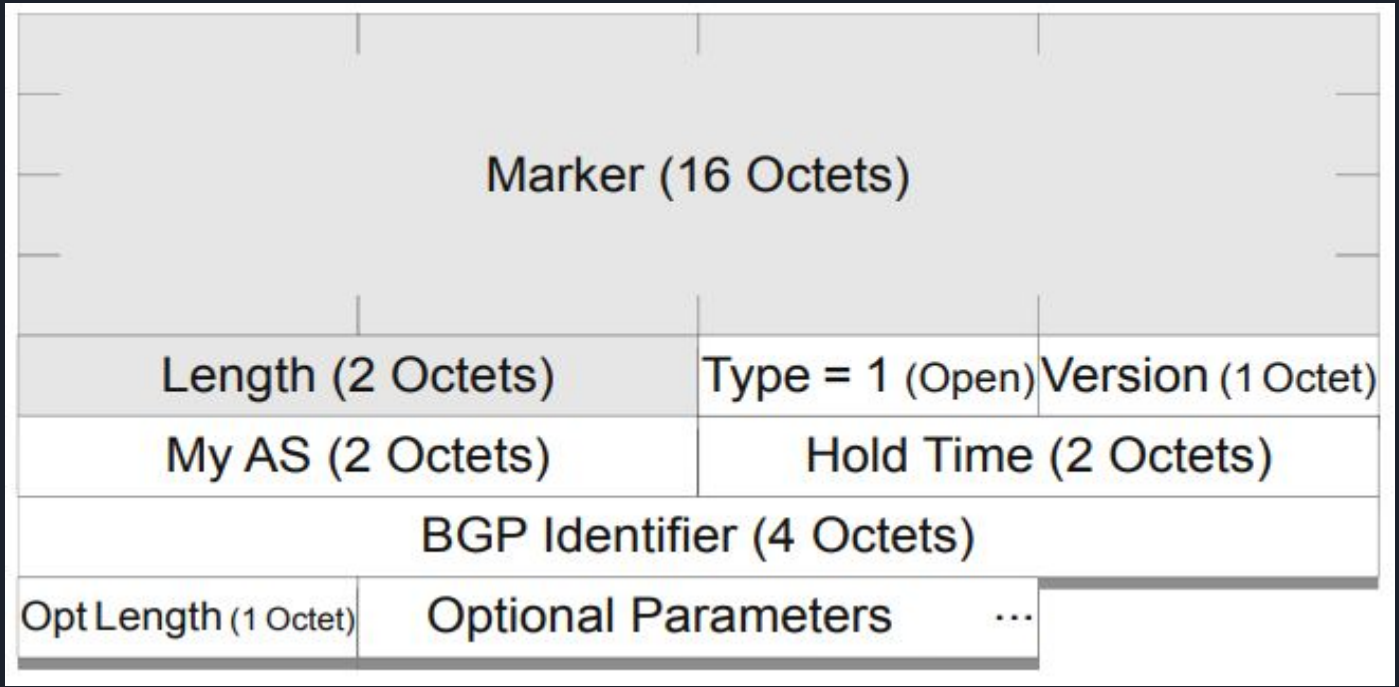


Figure. BGP Header

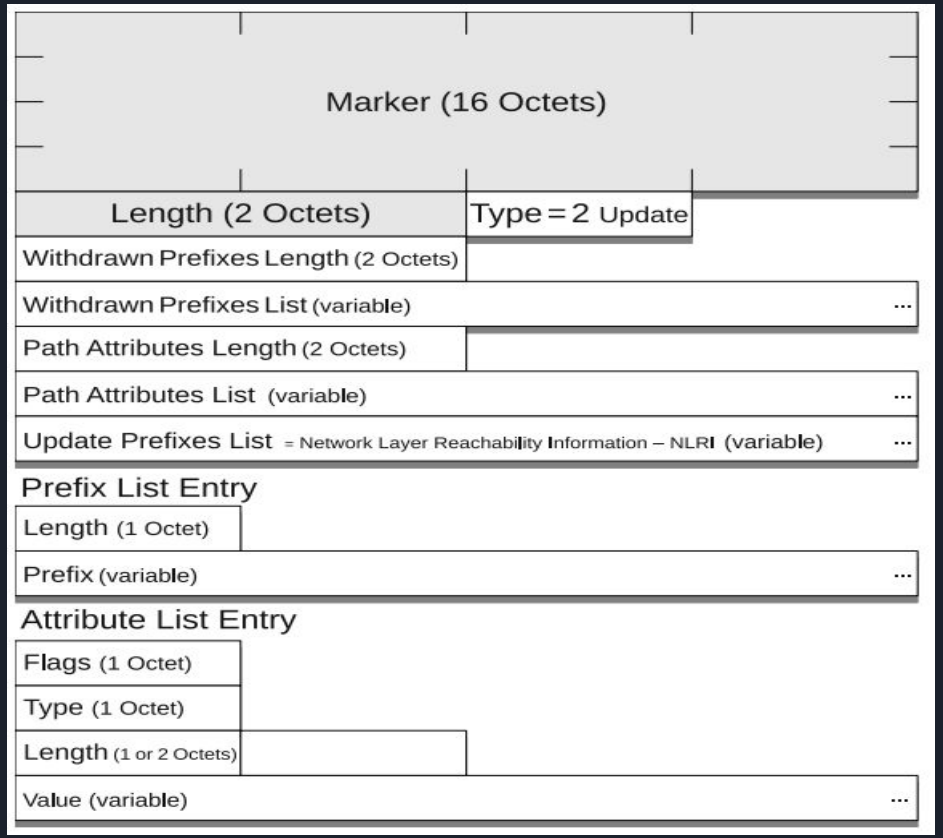
BGP Open Message

BGP uses an explicit open message to commence a BGP peering session.



BGP Update Message

For every UPDATE it receives, a BGP router should be able to verify that the “owner” of each prefix authorized the first (origin) AS to advertise the prefix and that each subsequent AS in the path has been authorized by the preceding AS to advertise a route to the prefix



Other BGP Messages

- **Keep-alive message**: Testing if a BGP peer is steel reachable
- **Notification message**: signal an error in BGP session

BGP Issues & Vulnerabilities

TCP Vulnerabilities

- **TCP Synchronization**: A BGP peer cannot verify the BGP peer's identity that is requesting the establishment of the session.
- **TCP Acknowledgement**: It can be spoofed by an outsider to be connected with a BGP peer and receives all BGP messages which contain all routing information.
- **TCP Reset**: the receipt of a TCP RST causes immediately the TCP session closure.

BGP Messages Vulnerabilities

BGP Header: any syntactic error in the BGP header can close the BGP session.

Open Message: If an open message is sent through an active session it could cause the session closure and could delete the BGP routes learned via this session.

Update Message: Any syntax error in any field of the received message may close the BGP session. Also, if the update message is received when the session is not yet established it causes the session's closure.

Keep-Alive Message: If the BGP node receives the keep-alive message, it switches to the idle state and the session is closed.

Notification Message: the reception of this message causes automatically the session's closure.

BGP Attacks

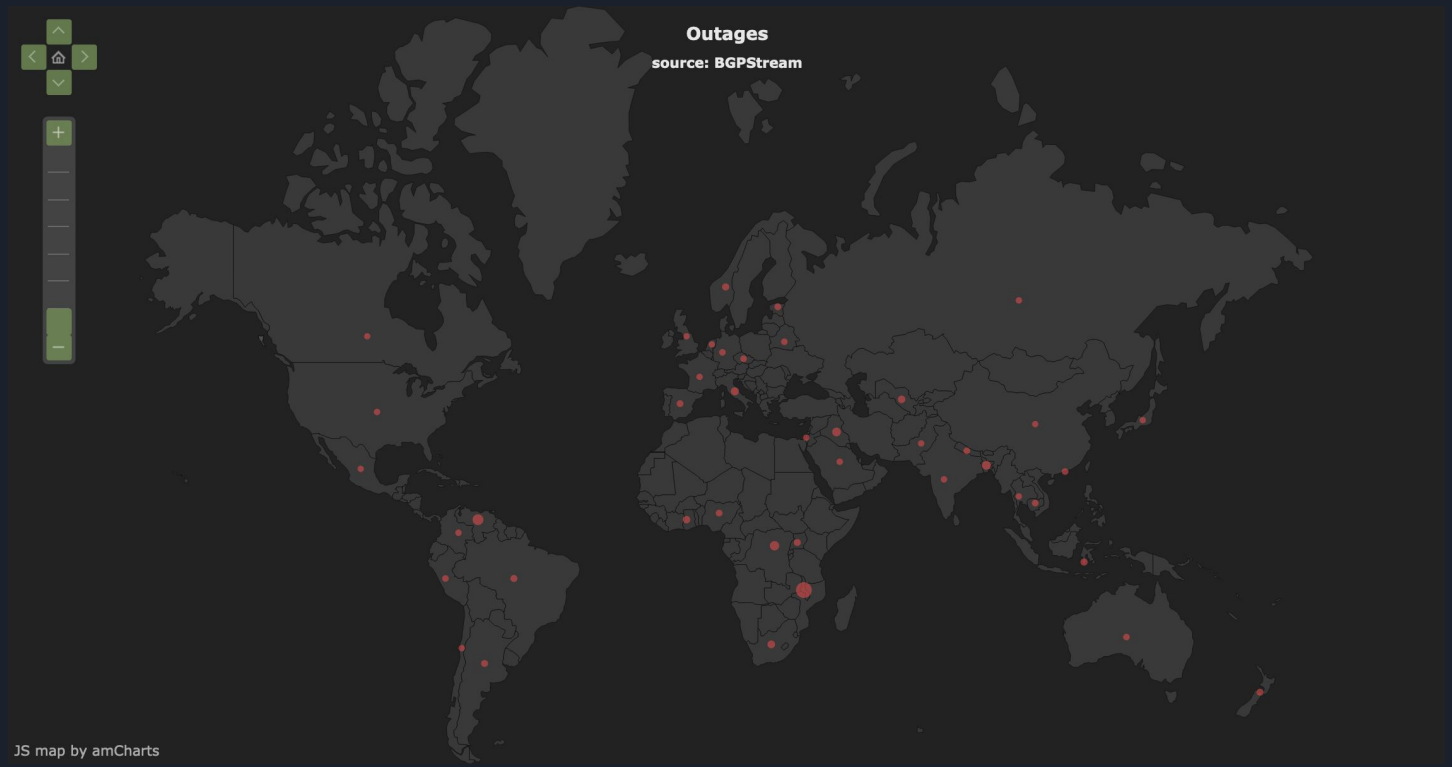
1) Confidentiality Attack - BGP routing information are sent in clear text over the peering session, thus any outsider can eavesdrop on the peering session and have access to routing information.

2) Message Deletion - an outsider can establish a connection with a BGP peer using the BGP vulnerabilities already explained. Then, he can delete the exchanged messages.

3) Man-in-the-Middle - Because of the absence of peers authentication in BGP, an outsider can easily stand between two peers and can intercept all exchanged messages.

4) Denial of Service - injecting large number of routes objects which can cause the saturation of the router's table and deny all BGP services.

BGP Attacks



Largest outage events with geographic distribution, March 2019 - bgpstream.com

Example of BGP Attacks

Example of BGP Attacks

DoS prevention

- **Generalized TTL Security Mechanism -** This technique relies on TTL that would prevent an attacker from effectively reaching the BGP process on a router with forged packets
- Make the interfaces on which the BGP session is running completely unreachable from outside the local network or the local segment. Using link-local addresses in IPv6.
- link-local address is an IPv6 unicast address that refer only to a particular physical link
- Applying packet-filters on the relevant address ranges at the network edge

Secure-BGP

- S-BGP is an architectural solution to the BGP security problems described earlier
- S-BGP represents an extension of BGP
- it uses a standard BGP facility to carry additional data about paths in UPDATE messages
- It adds an additional set of checks to the BGP route selection algorithm

S-BGP Main Mechanisms

Public Key Infrastructures (PKI) Certificates - *allows a BGP speaker to authenticate all routing information*

- S-BGP uses two PKI's, the first one is used to authenticate address allocations, and the second one is used to bind AS numbers to organizations, and organizations to routers in their networks.

- All messages sent by a BGP peer are signed with associated private key, and the receiver BGP peer verify, using the two PKI's

S-BGP Main Mechanisms

Route Attestations

- New path attribute included in the update message
- Each AS must have an attestation which indicates that it's authorized to advertise routes to the IP destination
- This attestation allows the BGP speaker to assert the authenticity of the BGP speaker sending the update message, and of the advertised routes

S-BGP Main Mechanisms

IPSecurity (IPSEC)

- S-BGP uses IPSec for verifying the BGP messages integrity, and the speaker sender identity

- IPsec protects the BGP traffic against several types of attacks including attacks related to TCP

Conclusion

- BGP is an essential part of the Internet needed to route traffic
- BGP is just like GPS for packets
- BGP is highly exposed to false route advertisements and other vulnerabilities
- S-BGP provides a way to protect against many problems

References

- https://www.incapsula.com/blog/bgp-routing-explained.html
- http://www.enterprisenetworkingplanet.com/netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm
- https://security.stackexchange.com/questions/56069/what-security-mechanisms-are-used-in-bgp-and-why-do-they-fail
- https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-25/securing-bgp-s-bgp.html
- https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/
- http://www.ciscopress.com/articles/article.asp?p=1237179&seqNum=2
- https://www.networkcomputing.com/networking/bgp-security-no-quick-fix
- https://www.cisco.com/c/en/us/about/security-center/protecting-border-gateway-protocol.html
- https://www.bgp4.as/security
- https://en.wikipedia.org/wiki/Border_Gateway_Protocol
- https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf
- https://www.cs.purdue.edu/truselab/readings/ripe45-eof-stephen.pdf
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5473881&tag=1