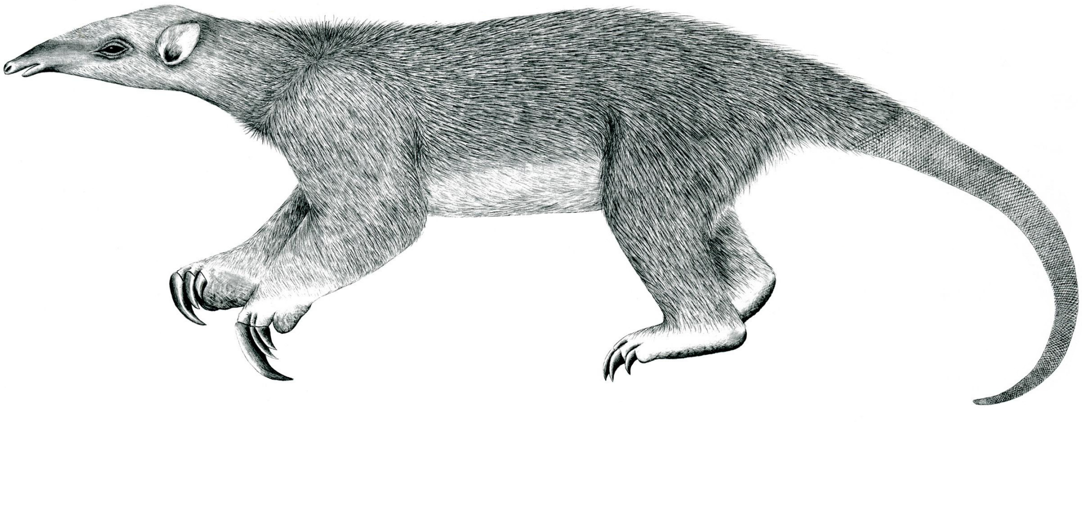
Tranalyzer2

bgpDecode

Border Gateway Protocol (BGP)



Tranalyzer Development Team

Contents

1 bgpDecode **1**
1.1 Description . . . 1
1.2 Dependencies . . . 1
1.3 Configuration Flags . . . 1
1.4 Flow File Output . . . 2
1.5 Additional Output . . . 7
1.6 Plugin Report Output . . . 8
1.7 Post-Processing . . . 8
1.8 Anomalies . . . 12
1.9 Examples . . . 12
1.10 References . . . 13

1 bgpDecode

1.1 Description

The bgpDecode plugin analyzes BGP traffic.

1.2 Dependencies

None.

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
`BGP_DEBUG`	0	Activate debug output
`BGP_IP_FORMAT`	1	IP addresses representation: 0: hex, 1: IP, 2: int
`BGP_AS_FORMAT`	0	AS number representation: 0: ASPLAIN, 1: ASDOT, 2: ASDOT+
`BGP_NOTIF_FORMAT`	0	Notifications representation: 0: uint8, 1: string (code only), 2: string (code and subcode) (not implemented)
`BGP_TRAD_BOGONS`	1	Flag traditional bogons
`BGP_RT`	1	Store routing information in a hashtable (required for MOAS detection)
`BGP_DEBUG_RT`	0	Activate debug output for routing information
`BGP_OUTPUT_RT`	1	Output routing tables
`BGP_RT_MASK`	0	Use the mask as part of the key for the routing table
If `BGP_OUTPUT_RT=1` then the following flags can be used:		
`BGP_ORIG_ID`	0	Output originator id
`BGP_AGGR`	0	Output aggregator
`BGP_CLUSTER`	0	Output cluster list
`BGP_COMMUNITIES`	0	Output communities
`BGP_MASK_FORMAT`	1	Netmask representation: 0: hex, 1: IP, 2: int
`BGP_AS_PATH_AGGR`	0	Aggregate repetitions of the same AS
`BGP_ASIZE`	255	Size of arrays for update records

Name	Default	Description
BGP_SUFFIX	"_bgp.txt"	Suffix to use for routing table information
BGP_ANOM_SUFFIX	"_bgp_anomalies.txt"	Suffix for anomaly file
BGP_MOAS_SUFFIX	"_bgp_moas.txt"	Suffix for multiple origin AS (MOAS) file

1.3.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- BGP_SUFFIX
- BGP_ANOM_SUFFIX
- BGP_MOAS_SUFFIX

1.4 Flow File Output

The bgpDecode plugin outputs the following columns:

Column	Type	Description	Flags
bgpStat	H16	BGP status	
bgpAFlgs	H16	BGP anomalies	
bgpMsgT	H8	BGP message types	
bgpNOpen_	U32_	Number of BGP OPEN messages,	
Upd_	U32_	UPDATE messages,	
Notif_	U32_	NOTIFICATION messages,	
KeepAl_	U32_	KEEPALIVE messages,	
RteRefr	U32	ROUTE-REFRESH messages	
bgpVersion	U8	BGP version	
bgpSrcAS_dstAS	U32_U32	Source and destination AS	BGP_AS_FORMAT=0
bgpSrcAS_dstAS	SC_SC	Source and destination AS	BGP_AS_FORMAT>0
bgpSrcId_dstId	IP_IP	Source and destination BGP ID	BGP_IP_FORMAT=0
bgpSrcId_dstId	U32_U32	Source and destination BGP ID	BGP_IP_FORMAT=1
bgpSrcId_dstId	H32_H32	Source and destination BGP ID	BGP_IP_FORMAT=2
bgpHTime	U16	BGP hold time (sec)	
bgpCaps	H16	Capabilities	
bgpPAttr	H32	Path attributes	
bgpNAdver	U32	Total number of advertised routes	
bgpNWdrwn	U32	Total number of withdrawn routes	
bgpMaxAdver	U32	Max. num. of advertised routes per record	
bgpAvgAdver	D	Average num. of advertised routes per record	
bgpMaxWdrwn	U32	Max. num. of withdrawn routes per record	
bgpAvgWdrwn	D	Average num. of withdrawn routes per record	
bgpAdvPref	H32	Advertised prefixes	
bgpWdrnPref	H32	Withdrawn prefixes	
bgpNIGP_	U32_	Number of routes from origin IGP	

Column	Type	Description	Flags
EGP_	U32_	EGP,	
INC	U32	INCOMPLETE	
bgpMinASPLen	U8	Minimum AS path length	
bgpMaxASPLen	U8	Maximum AS path length	
bgpAvgASPLen	D	Average AS path length	
bgpMaxNPrepAS	U32	Maximum number of prepended AS	
bgpMinIatUp	D	Minimum inter-arrival time for update	
bgpMaxIatUp	D	Maximum inter-arrival time for update	
bgpAvgIatUp	D	Average inter-arrival time for update	
bgpMinIatKA	D	Minimum inter-arrival time for keep-alive	
bgpMaxIatKA	D	Maximum inter-arrival time for keep-alive	
bgpAvgIatKA	D	Average inter-arrival time for keep-alive	
bgpNotifCode_Subcode	U8_U8	Notification (fatal error) code and subcode	BGP_NOTIF_FORMAT=0
bgpNotifCode_Subcode	SC_U8	Notification (fatal error) code and subcode	BGP_NOTIF_FORMAT=1

1.4.1 bgpStat

The bgpStat column is to be interpreted as follows:

bgpStat	Description
0x0001	Flow is BGP
0x0002	Connection Not Synchronized
0x0004	Bad Message Length
0x0008	Bad Message Type
0x0010	Unsupported Version Number
0x0040	Unacceptable Hold Time
0x0080	Invalid network mask (> 32)
0x0100	Inter-arrival time for update or keep-alive < 0
0x0200	AS Mismatch
0x0400	Atomic Aggregate
0x4000	One of the array was full... increase BGP_ASIZE
0x8000	Malformed packet (snapped or segmented)

1.4.2 bgpAFlgs

The bgpAFlgs column is to be interpreted as follows:

bgpAFlgs	Description
0x0001	Bogons advertisement
0x0002	Prefix more specific than /24 was advertised
0x0004	Prefix less specific than /8 was advertised

bgpAFlgs	Description
`0x0008`	Possible blackhole: community with tag 666
`0x0010`	Possible loop: My AS in AS path
`0x0020`	Multiple Origin AS (same prefix announced by more than one origin AS)
`0x0040`	AS prepended more than 10 times in AS path
`0x0080`	AS number reserved for private use in AS path (AS: 64512-65534, AS4: 4200000000-4294967294)
`0x0100`	Route for more specific prefix advertised

1.4.3 bgpMsgT

The `bgpMsgT` column is to be interpreted as follows:

bgpMsgT	Description
`0x01`	—
`0x02`	OPEN Message
`0x04`	UPDATE Message
`0x08`	NOTIFICATION Message
`0x10`	KEEPALIVE Message
`0x20`	ROUTE-REFRESH Message
`0x40`	—
`0x80`	—

1.4.4 bgpHTime

The `bgpHTime` column indicates the number of seconds which can elapse without receiving a message. It should be three times the frequency of keep-alive messages (the default is to send one keep-alive message every 30 seconds, thus having a hold-time of 90s). Common values for the `bgpHTime` column are:

bgpHTime	Description
0	Infinite hold-time (no keep-alive messages are sent)
1,2	Illegal values
3	Minimum legal value
< 20	Warning: A hold-time of less than 20 seconds increases the chances of peer flapping
90	Juniper
180	Cisco

1.4.5 bgpCaps

The `bgpCaps` column is to be interpreted as follows:

bgpCaps	Description
0x0001	Multiprotocol Extensions for BGP-4
0x0002	Route Refresh Capability for BGP-4
0x0004	Outbound Route Filtering Capability
0x0008	Multiple routes to a destination capability
0x0010	Extended Next Hop Encoding
0x0020	Graceful Restart Capability
0x0040	Support for 4-octet AS number capability
0x0080	Support for Dynamic Capability (capability specific)
0x0100	Multisession BGP Capability
0x0200	ADD-PATH Capability
0x0400	Enhanced Route Refresh Capability
0x0800	Long-Lived Graceful Restart (LLGR) Capability
0x1000	FQDN Capability
0x8000	Unhandled Capability, i.e., none of the above

1.4.6 bgpPAttr

The bgpPAttr column is to be interpreted as follows (bold attributes are mandatory, attributes in italic are deprecated):

bgpPAttr	Description
0x00000001	**ORIGIN**
0x00000002	**AS_PATH**
0x00000004	**NEXT_HOP**
0x00000008	MULTI_EXIT_DISC (MED)
0x00000010	LOCAL_PREF
0x00000020	ATOMIC_AGGREGATE
0x00000040	AGGREGATOR
0x00000080	COMMUNITIES
0x00000100	ORIGINATOR_ID
0x00000200	CLUSTER_LIST
0x00000400	DPA (Designation Point Attribute)
0x00000800	ADVERTISER
0x00001000	RCID_PATH / CLUSTER_ID
0x00002000	MP_REACH_NLRI
0x00004000	MP_UNREACH_NLRI
0x00008000	EXTENDED_COMMUNITIES

bgpPAttr	Description
0x00010000	NEW_AS_PATH
0x00020000	NEW_AGGREGATOR
0x00040000	*SSA, SAFI Specific Attribute*
0x00080000	Connector Attribute
0x00100000	*AS_PATHLIMIT*
0x00200000	PMSI_TUNNEL
0x00400000	Tunnel Encapsulation Attribute
0x00800000	Traffic Engineering
0x01000000	IPv6 Address Specific Extended Community
0x02000000	–
0x04000000	PE Distinguisher Labels

1.4.7 bgpAdvPref and bgpWdrnPref

The `bgpAdvPref` and `bgpWdrnPref` columns are to be interpreted as follows:

bgpAdvPref	Description
`0x00000001`	/1
`0x00000002`	/2
`0x00000004`	/3
`0x00000008`	/4
`0x00000010`	/5
`0x00000020`	/6
`0x00000040`	/7
`0x00000080`	/8
`0x00000100`	/9
`0x00000200`	/10
`0x00000400`	/11
`0x00000800`	/12
`0x00001000`	/13
`0x00002000`	/14
`0x00004000`	/15
`0x00008000`	/16
`0x00010000`	/17
`0x00020000`	/18
`0x00040000`	/19
`0x00080000`	/20
`0x00100000`	/21
`0x00200000`	/22
`0x00400000`	/23
`0x00800000`	/24
`0x01000000`	/25
`0x02000000`	/26
`0x04000000`	/27
`0x08000000`	/28
`0x10000000`	/29
`0x20000000`	/30
`0x40000000`	/31
`0x80000000`	/32

1.4.8 bgpNotifCode_Subcode

The `bgpNotifCode_Subcode` column is to be interpreted as follows:

Code	Subcode	Description
1		Message Header Error
	1	Connection Not Synchronized
	2	Bad Message Length
	3	Bad Message Type
2		OPEN Message Error
	1	Unsupported Version Number
	2	Bad Peer AS
	3	Bad BGP Identifier
	4	Unsupported Optional Parameter
	5	Deprecated
	6	Unacceptable Hold time
	7	Unsupported capability
3		UPDATE Message Error
	1	Malformed Attribute List
	2	Unrecognized Well-known Attribute
	3	Missing Well-known Attribute
	4	Attribute Flags Error
	5	Attribute Length Error
	6	Invalid ORIGIN Attribute
	7	Deprecated

Code	Subcode	Description
	8	Invalid NEXT_HOP Attribute
	9	Optional Attribute Error
	10	Invalid Network Field
	11	Malformed AS_PATH
4		Hold Timer Expired (no subcode)
5		Finite State Machine Error
	1	Receive Unexpected Message in OpenSent State
	2	Receive Unexpected Message in OpenConfirm State
	3	Receive Unexpected Message in Established State
6		Cease
	1	Maximum Number of Prefixes Reached
	2	Administrative Shutdown
	3	Peer De-configured
	4	Administrative Reset
	5	Connection Rejected
	6	Other Configuration Change
	7	Connection Collision Resolution
	8	Out of Resources
7		ROUTE-REFRESH Message Error
	1	Invalid Message Length

1.5 Additional Output

If `BGP_OUTPUT_RT=1`, then a `PREFIX_bgp.txt` file is created. Note that the suffix can be configured with `BGP_SUFFIX`. This file uses the configuration options defined in Section 1.3.

Column	Type	Description	Flags
`NLRI`	R(S)	Target network	
`AS`	U32/S	Originating AS	`BGP_AS_FORMAT`
`NextHop`	IP4	Next hop	
`MED`	U32	Multi Exit Discriminator (MED)	
`LocPref`	U32	Local Preference	
`Origin`	S	Origin (IGP, EGP, INCOMPLETE, UNKNOWN)	
`OriginatorID`	IP4	Originator ID	`BGP_ORIG_ID=1`
`OriginAS`	R(U32)	Origin AS	
`UpstreamAS`	R(U32)	Upstream AS	
`DestAS`	U32	Destination AS	
`Aggregator`	S	Aggregator (AS:Origin)	`BGP_AGGR=1`
`ASPath`	S	List of AS to visit to reach target network	
`ASPathLen`	U32	Length of the AS path	
`MaxNPrepAS`	U32	Maximum number of prepended AS	

Column	Type	Description	Flags
`ClusterList`	R(IP4)	Cluster list	`BGP_CLUSTER=1`
`ClusterListLen`	U32	Cluster list length	`BGP_CLUSTER=1`
`Communities`	R(S)	List of communities (AS:tag)	`BGP_COMMUNITIES=1`
`WithdrawnRoutes`	R(S)	List of withdrawn routes	
`flowInd`	U64	Flow index of the advertisement	
`pktNo`	U64	Packet index of the advertisement	
`RecNum`	U64	Record index (within the packet) of the advertisement	
`time`	U32	Timestamp of the advertisement	

1.6 Plugin Report Output

The number of BGP packets and OPEN, UPDATE, NOTIFICATION, KEEP-ALIVE and ROUTE-REFRESH messages is reported. In addition, the aggregated `bgpAFlgs` anomalies are reported.

1.7 Post-Processing

1.7.1 bgpR

The `bgpR` script creates a `PREFIX_bgp_s.txt` file, which is similar to the input file, but easier to process. The target networks are split and sorted, redundant records are omitted and the list of countries and continents to visit to reach the target network is added (`ASPathCountries` and `ASPathContinents`).

In addition, the following files are created:

- `PREFIX_bgp_mpath.txt`: outputs, for all networks which have more than one path, the number of distinct paths.
- `PREFIX_bgp_conf.txt`: lists possible configuration errors, e.g., an AS number prepended *N* times, followed by AS number *N*.

The script can also be used to plot AS paths between AS numbers, countries and continents (Figure 1).

Usage:
The `bgpR` script uses the `PREFIX_bgp.txt` file described in Section 1.5 as input: `./bgpR PREFIX_bgp.txt`
For a complete list of options, use the `-h` or `--help` option: `bgpR --help`.

Plot Configuration:
To color specific countries, edit the `bgpR` script (search for *colorN*), by adding a case for the missing country or by changing the color. For example, to color Switzerland in red, add the following line in the switch:

```
case "CH": color = "red"; break;
```

For the coloring of the edges, search for *cstr* and edit the semi-colon separated string. A complete list of colors can be found at `http://www.graphviz.org/doc/info/colors.html`.

1.7.2 ASPathCountries

For a list of countries, refer to `countrycodes.txt` in the doc folder.

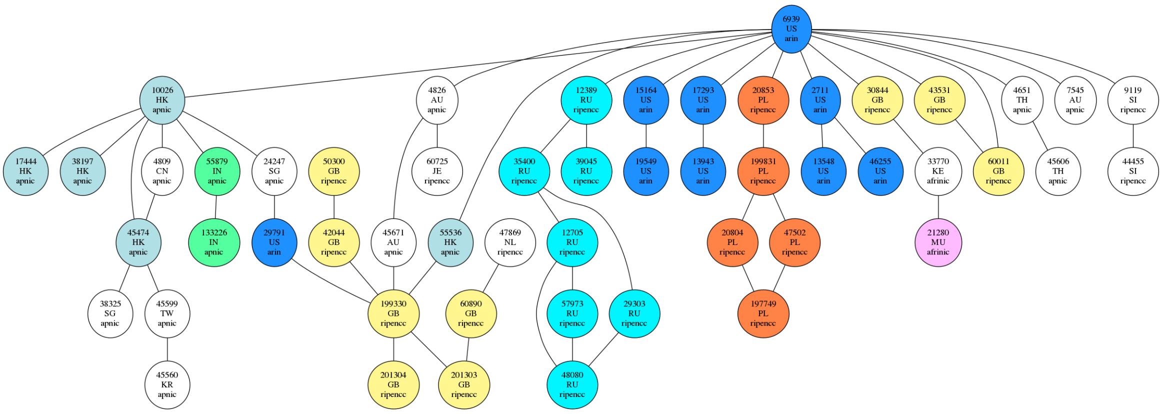


Figure 1: *Paths between AS*

1.7.3 ASPathContinents

The `ASPathContinents` column is to be interpreted as follows:

ASPathContinents	Description
afrinic	Africa Region
apnic	Asia/Pacific Region
arin	Canada, USA and some Caribbean Islands
ietf	Reserved/Unknown
lacnic	Latin America and some Caribbean Islands
ripencc	Europe, the Middle East and Central Asia

ARIN
RIPE NCC
AFRINIC
APNIC
LACNIC

1.7.4 bgp2ng

The bgp2ng script can be used to generate plots similar to bgpR but readable by netgraph (Figure 2). It uses the PREFIX_bgp_s.txt file described in Section 1.7.1 as input:

```
./bgp2ng PREFIX_bgp_s.txt
```

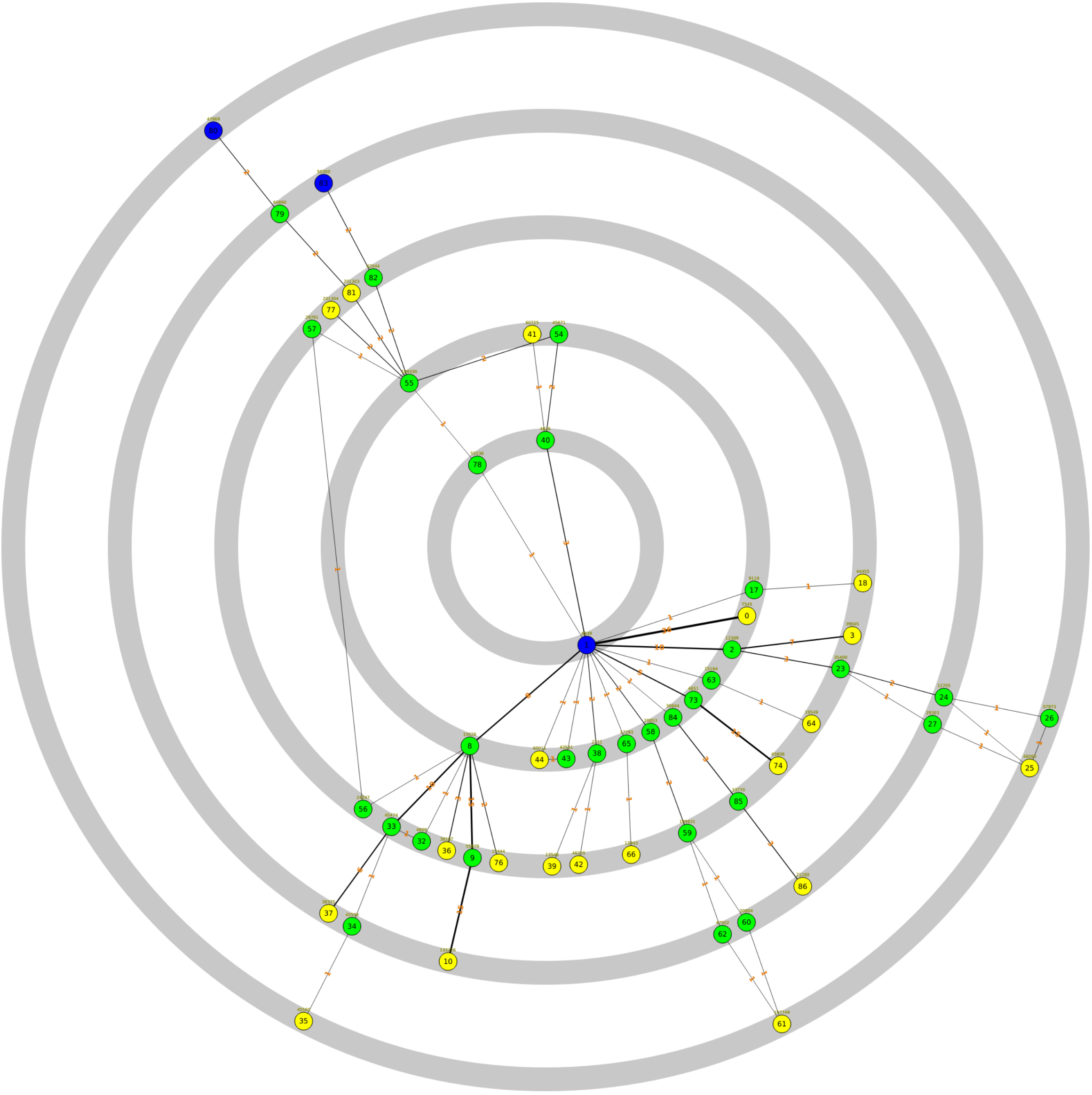


Figure 2: *Paths between AS*

It creates the following files:

- PREFIX_bgp_netgraph0.txt: connections between network and next hop

- `PREFIX_bgp_netgraph1.txt`: connections between first and last AS
- `PREFIX_bgp_netgraph2.txt`: connections between all AS
- `PREFIX_bgp_netgraph3.txt`: connections between first and last country
- `PREFIX_bgp_netgraph4.txt`: connections between all countries
- `PREFIX_bgp_netgraph5.txt`: connections between first and last continent
- `PREFIX_bgp_netgraph6.txt`: connections between all countries
- `PREFIX_bgp_netgraph7.txt`: connections between network, next hop, first and last AS, country and continent, ASPath

1.7.5 bgpMOAScn

The `bgpMOAScn` script adds information regarding the country of the multiple origins AS (MOAS) reported in the file `FILE_moas.txt`. Save the results in `FILE_moas_cn.txt`. Use `bgpMOAScn -h` for more information. Note that it is best to validate the countries using `whois` on the AS number and network to ensure the information is up to date, e.g., `whois AS1234` or `whois 1.2.3.4/24`.

1.8 Anomalies

Anomalies are summarized in the `bgpAFlgs` columns and in `FILE_bgp_anomalies.txt`.

- Bogons advertisement:
  `awk '/^BOGON/' FILE_bgp_anomalies.txt`
- Prefix more specific than /24:
  `awk '/^SPEC24/' FILE_bgp_anomalies.txt`
- Prefix less specific than /8:
  `awk '/^SPEC8/' FILE_bgp_anomalies.txt`
- Possible blackhole:
  `awk '/^BLACKHOLE/' FILE_bgp_anomalies.txt`
- Possible loop:
  `awk '/^LOOP/' FILE_bgp_anomalies.txt`
- Multiple Origin AS (MOAS) are reported in `FILE_moas.txt` (see also `bgpMOAScn`)
- AS number prepended more than 10 times in AS path:
  `awk '/^NPREPAS/' FILE_bgp_anomalies.txt`
- Private/Reserved AS numbers:
  `awk '/^PRIVAS/' FILE_bgp_anomalies.txt`
- More specific prefix to existing network:
  `awk '/^MSPEC/' FILE_bgp_anomalies.txt`

In addition, the number of distinct paths (if bigger than one) to reach a specific network is summarized in the file `FILE_bgp_mpath.txt` along with some statistics regarding the different AS path lengths (minimum, maximum, range, mean, median, standard deviation and mode). The file also highlights whether a MOAS was detected for the network. Possible misconfigurations are reported in `FILE_bgp_conf.txt`. Note that the last two files are created by the `bgpR` script.

1.9 Examples

- BGP flows can be extracted from a flow file by using the `bgpStat` column as follows:

```
tawk 'hdr() || strtonum($bgpStat)' FILE_flows.txt
```

- BGP flows with anomalies can be extracted from a flow file by using the `bgpAFlgs` column as follows:

```
tawk 'hdr() || strtonum($bgpAFlgs)' FILE_flows.txt
```

- More details about the anomalies listed in FILE_bgp_anomalies.txt can be found by using the flowInd, pktNo and RecNum columns and FILE_bgp_s.txt or FILE_bgp.txt files as follows, e.g., for flowInd=1, pktNo=2 and RecNum=3 (note that tawk flow and packet functions could also be used):

  ```
  tawk '$flowInd == 1 && $pktNo == 2 && $RecNum == 3' FILE_bgp_s.txt
  ```

  Alternatively, the following command can be used to achieve similar results:

  ```
  grep -P "1\t2\t3" FILE_bgp_s.txt
  ```

- Display the 10 networks which experienced the most more specific prefix advertisements:

  ```
  tawk '/^MSPEC/ { a[$ASorNet]++ } END { for (i in a) print i, a[i] }'
            FILE_bgp_anomalies.txt | sort -nrk2 | head -10
  ```

- To plot the AS paths for a specific network, proceed as follows:

  1. Run the bgpR script: bgpR FILE_bgp.txt
  2. Run the bgp2ng script: bgp2ng FILE_bgp_s.txt
  3. Use tawk as follows, e.g., to keep network 123.123.123.0/24 only:

  ```
  tawk '
      hdr() {
          printf "%s\t%s\t%s\n", chomp($0), "ASP1", "ASP2"
          next
      }

      $NLRI ~ /^123\.123\.123\.0\/24$/ {
          l = split($ASPath, asp, ";")
          for (i = 1; i < l; i++) {
             printf "%s\t%s\t%s\n", chomp($0), asp[i], asp[i+1]
          }
      }
  ' FILE_bgp_netgraph7.txt
  ```

  4. Open the file with Traviz/Netgraph

1.10 References

- RFC4271: A Border Gateway Protocol 4 (BGP-4)
- IPv4 traditional bogons list
- https://www.iana.org/assignments/