Quick Note 9

Configuring the BGP file (bgp.conf)

Digi Technical Support

February 2016

1 INTRODUCTION

This Quick Note explains the syntax used in the BGP configuration file in more detail. There are also details of debug commands for troubleshooting.

1.1 Version

	Status
1.0	Published
2.0	Updated and rebranded
2.1	Updated for new GUI
2.2	Updated screenshots and instructions for new web interface, rebranding (Feb 2016)

2 CONFIGURATION

There are two parts to configuring BGP on a TransPort. The first section deals with the configuration of the BGP daemon via a configuration file. The second section deals with the BGP configuration settings on the web interface.

2.1 Configuration file

The configuration of BGP on a TransPort is held in a separate text file, usually named *bgp.conf*. This file will need to be manually created using a text editor then placed on to the TransPort via FTP for example.

Below is an example *bgp.conf* file with 2 areas. An interface can only exist in one area. A '#' symbol is used to denote a comment; as can be seen from the example, there are three distinct sections to the config file.

```
#macros

# global configuration
AS 65001
router-id 10.0.0.3
holdtime 180
holdtime min 3
log updates
network 10.0.0.0/28

#neighbours

neighbor 10.0.0.1 {
        remote-as       65001
        descr           MW1
        depend on       ppp1
        set nexthop self
        announce        all
}
neighbor 10.0.0.2 {
        remote-as       65001
        descr           MW2
        depend on       eth1
        set nexthop self
        announce        all
}
neighbor 172.16.0.2 {
        remote-as       65002
        descr           REM-01
         depend on  tun0
        announce        self
}

#BGP route Filters
#These filters are optional and are shown as examples of what could be used

#deny to any prefix 172.16.0.0/12 prefixlen >= 12

# filter out prefixes longer than 24 or shorter than 8 bits
#deny from any
#allow from any prefixlen 8 - 24

# do not accept a default route
#allow from any prefix 0.0.0.0/0

# filter bogus networks
#deny from any prefix 10.0.0.0/8 prefixlen >= 8
#deny from any prefix 172.16.0.0/12 prefixlen >= 12
#deny from any prefix 192.168.0.0/16 prefixlen >= 16
#deny from any prefix 169.254.0.0/16 prefixlen >= 16
#deny from any prefix 192.0.2.0/24 prefixlen >= 24
#deny from any prefix 224.0.0.0/4 prefixlen >= 4
#deny from any prefix 240.0.0.0/4 prefixlen >= 4
```

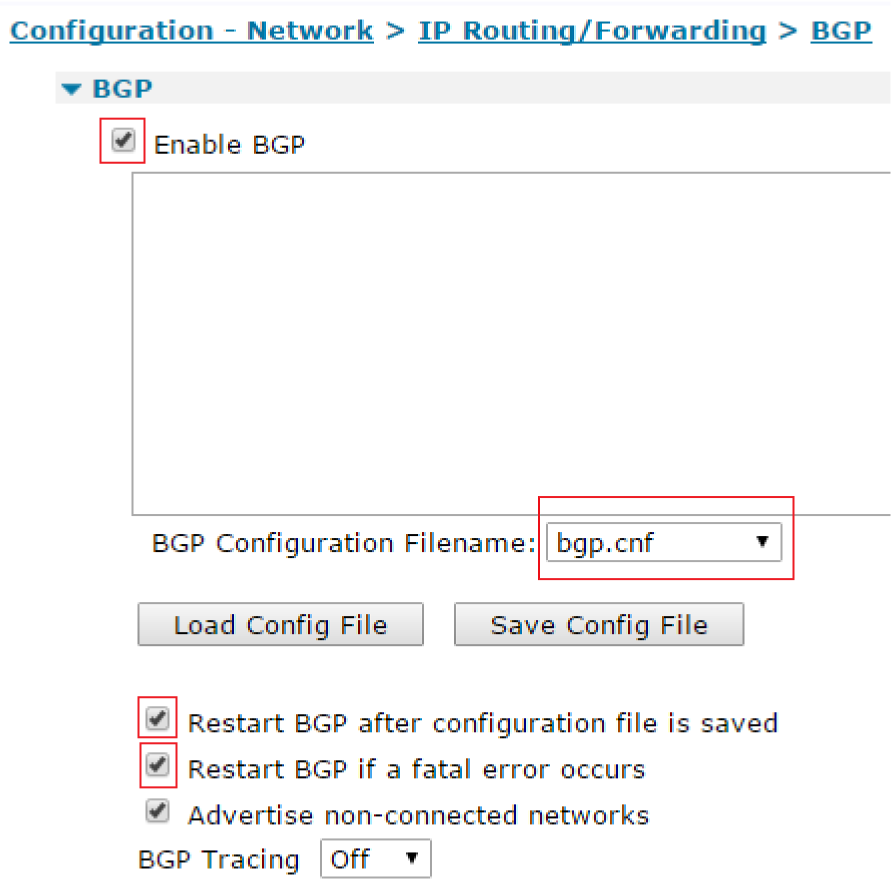
The sections are:

- **Macros** – These are user defined variables that set values of parameters used in the rest of the configuration.
- **Global configuration** – Any of the area or interface configuration option can be set to a default value here to help simplify the configuration.
- **Neighbours** – At least one area must exist. An area groups interfaces together. Any parameters set in the areas will override any global options. Valid interfaces are ethx, pppx and tunx, where the x is the interface number.
- **Filters** – The final section contains the filters that are applied to inbound and outbound routing updates.

Please see section 4 for a complete list of all available commands and their functions.

2.2 Web interface configuration

There is also a small amount of setup required, in the TransPort's web interface. This can be found by navigating to the following section:



Configuration - Network > IP Routing/Forwarding > BGP

▼ BGP

☑ Enable BGP

BGP Configuration Filename: bgp.cnf ▼

☑ Restart BGP after configuration file is saved

☑ Restart BGP if a fatal error occurs

☑ Advertise non-connected networks

BGP Tracing Off ▼

The 'BGP Tracing' option, which is Off by default, may be used to ensure that BGP is configured and running correctly and help troubleshoot BGP issues. The corresponding CLI commands are as follows:

Off = bgp 0 debug off

Low = bgp 0 debug on

Med = bgp 0 debug 2

High = bgp 0 debug 3

To view the debug output, first connect to the TransPort via a serial or Telnet. If using serial, type `‘debug x’` *(where x is the ASY port number, e.g. 0, 1, 2 or 3).* If using Telnet, type `’debug t’`. All of the BGP debug information will now be displayed in the terminal window.

Once you are satisfied that BGP is configured and running correctly, turn Off BGP Tracing, type `’debug off’` in the CLI, and then disable and re-enable BGP.

3 USING TEXT COMMANDS

There are a number of CLI commands for checking the status of the BGP routing process. The commands and their functions are listed below

- **bgpctl show interface** – Lists all of the interfaces on the TransPort and their status within BGP, i.e. if they are up or down.
- **bgpctl show network** – Displays a list of the networks which are connected to the TransPort that BGP knows about.
- **bgpctl show rib <*options*>** – Displays the Routing Information Base (rib) table, which holds all of the available routes on the router. There maybe duplicate routes to the same destination in this table.
- **bgpctl show fib <*connected / static / bgp / nexthop / x.x.x.x*>**– Displays the Forward Information Base (fib) table. This table holds the routes which the TransPort will actually use to forward traffic, therefore there will be not duplicate routes held in this table. The options can be used to look at more specific routes.
- **bgpctl show neighbour** – Displays a list of the BGP neighbours that are connected to the LAN segments which are attached to the TransPort. The current state of each neighbour will also be displayed in the table.
- **bgpctl show ip bgp <*options*>**
- **<options>** – the options are as follows:
  - **address / len** – Displays information about a specific route. Use the detail option as well to see detailed information.
  - **as y** – Show all entries with as anywhere in the AS path.
  - **source-as** – Show all entries with *as* as rightmost AS.
  - **transit-as** – Show all entries with *as* anywhere but rightmost.
  - **empty-as** – Show all entries that are internal routes with no AS's in the AS path.
  - **summary** – This is the same as the **show summary** command.
  - **detail** – Displays additional detail when used with one of the other options in this list
    - Example: Bgpctl show ip bgp **detail** as 65001
  - **memory** – Show BGP memory statistics.
- **bgpctl neighbor x.x.x.x <*Up / Down / Clear*> -** Allows a neighbour to be set to up or down manually or cleared, which will restart a new session with a neighbour.
- **bgpctl fib <*Couple / Decouple*>** - When coupled (default), BGP routes will be placed in the Sroute table. When Decoupled, routes will be learnt and placed in the BGP routing table but not placed in the Sroute table.
- **bgpctl network <options>**
  - **add** – Add the specified prefix to the list of announced networks.
  - **delete** – Remove the specified prefix from the list of announced networks.

  - **flush** – Remove all dynamically added prefixes from the list of announced networks.
  - **show** – Show all announced networks.

It is also worth checking the routing table via the web interface, or the command line interface (CLI).

- **route print** – Displays the entries in the routing table, shows networks that are attached to interfaces, static routes but also it will include routes learned dynamically from both BGP and OSPF.

4 LIST OF THE BGP.CONF PARAMETERS

```
The bgp.conf config file is divided into four main sections.

     Macros
           User-defined variables may be defined and used later, simplifying
           the configuration file.

     Global Configuration
           Global settings for bgp.

     Neighbors and Groups
           bgpd establishes sessions with neighbors.  The neighbor defini-
           tion and properties are set in this section, as well as grouping
           neighbors for the ease of configuration.

     Filter
           Filter rules for incoming and outgoing UPDATES.

     With the exception of macros, the sections should be grouped and appear
     in bgpd.conf in the order shown above.

Macros
     Macros can be defined that will later be expanded in context.  Macro
     names must start with a letter, and may contain letters, digits and un-
     derscores.  Macro names may not be reserved words (for example, AS,
     neighbor, or group).  Macros are not expanded inside quotes.

     For example:

           peer1="1.2.3.4"
           neighbor $peer1 {
                   remote-as 65001
           }

Global Configuration
     There are quite a few settings that affect the operation of the BGP
     daemon globally.

     AS as-number
             Set the local autonomous system number to as-number.  The AS num-
             bers are assigned by local RIRs, or a private as number.

             Private AS number are in the range 64512 to 65535

             For example:    AS 65001  sets the local AS to 65001.

     fib-update (yes|no)
             If set to no, do not update the Forwarding Information Base,
             a.k.a. the kernel routing table.  The default is yes.

     holdtime seconds
             Set the holdtime in seconds.  The holdtime is reset to its ini-
             tial value every time either a KEEPALIVE or an UPDATE message is
             received from the neighbor.  If the holdtime expires the session
             is dropped.  The default is 90 seconds.  Neighboring systems ne-
             gotiate the holdtime used when the connection is established in
             the OPEN messages.  Each neighbor announces its configured hold-
             time; the smaller one is then agreed upon.
```

```
holdtime min seconds
             The minimal accepted holdtime in seconds.  This value must be
             greater than or equal to 3.

     listen on address
             Specify the local IP address bgpd should listen on.

                   listen on 127.0.0.1

     log updates
             Log received and sent updates.

     network address/prefix [set ...]
     network static [set ...]
     network connected [set ...]
             Announce the specified network as belonging to our AS.  If set to
             connected, routes to directly attached networks will be an-
             nounced.  If set to static, all static routes will be announced.

                   network 192.168.7.0/24

             It is possible to set default AS path attributes per network
             statement:

                   network 192.168.7.0/24 set localpref 220

             See also the ATTRIBUTE SET section.

     nexthop qualify via (bgp|default)
             If set to bgp, BGP may use BGP routes to verify nexthops.  If
             set to default, bgp may use the default route to verify nex-
             thops.  By default bgp will only use static routes or routes
             added from the Sroute table.

     rde med compare (always|strict)
             If set to always, the MED attributes will always be compared.
             The default is strict, where the MED is only compared between
             peers belonging to the same AS.

     rde route-age (ignore|evaluate)
             If set to evaluate, the best path selection will not only be
             based on the path attributes but also on the age of the route,
             giving preference to the older, typically more stable, route.  In
             this case the decision process is no longer deterministic.  The
             default is ignore.

     route-collector (yes|no)
             If set to yes, the route selection process is turned off.  The
             default is no.

     router-id address
             Set the router ID to the given IP address, which must be local to
             the machine.

                   router-id 10.0.0.1

             If not given, the BGP ID is determined as the biggest IP address
             assigned to the local machine.
```

```
Neighbors
     BGP establishes TCP connections to other BGP speakers called
     neighbors.  Each neighbor is specified by a neighbor section, which al-
     lows properties to be set specifically for that neighbor:

           neighbor 10.0.0.2 {
                   remote-as 65002
                   descr "a neighbor"
           }

     Multiple neighbors can be grouped together by a group section.  Each
     neighbor section within the group section inherits all properties from
     its group:

           group "peering AS65002" {
                   remote-as 65002
                   neighbor 10.0.0.2 {
                           descr "AS65002-p1"
                   }
                   neighbor 10.0.0.3 {
                           descr "AS65002-p2"
                   }
           }

     Instead of the neighbor's IP address, an address/netmask pair may be giv-
     en:

           neighbor 10.0.0.0/8

     In this case, the neighbor specification becomes a template, and if a
     neighbor connects from an IP address within the given network, the tem-
     plate is cloned, inheriting everything from the template but the remote
     address, which is replaced by the connecting neighbor's address.  With a
     template specification it is valid to omit remote-as; bgpd will then
     accept any AS the neighbor presents in the OPEN message.

     There are several neighbor properties:

     announce (all|none|self|default-route)
             If set to none, no UPDATE messages will be sent to the neighbor.
             If set to default-route, only the default route will be announced
             to the neighbor.  If set to all, all generated UPDATE messages
             will be sent to the neighbor.  This is usually used for transit
             AS's and IBGP peers.  The default value for EBGP peers is self,
             which limits the sent UPDATE messages to announcements of the lo-
             cal AS.  The default for IBGP peers is all.

     announce (IPv4|IPv6) (none|unicast)
             For the given address family, control which subsequent address
             families (at the moment, only none, which disables the announce-
             ment of that address family, and unicast are supported) are an-
             nounced during the capabilities negotiation.  Only routes for
             that address family and subsequent address family will be an-
             nounced and processed.

     demote group
             Increase the carp demotion counter on the given interface
             group, usually carp, when the session is not in state
             ESTABLISHED.  The demotion counter will be increased as soon as
             bgpd(8) starts and decreased 60 seconds after the session went to
             state ESTABLISHED.  For neighbors added at runtime, the demotion
             counter is only increased after the session has been ESTABLISHED
```

```
        at least once before dropping.

        For more information on interface groups, see the group keyword
        in ifconfig(8).

depend on interface
        The neighbor session will be kept in state IDLE as long as
        interface reports no link.  This is primarily in-
        tended to be used with tunnel interfaces to reduce failover times.

        The state of the network interfaces on the system can be viewed
        using the show interfaces command to bgpctl.

descr description
        Add a description.  The description is used when logging neighbor
        events, in status reports, for specifying neighbors, etc., but
        has no further meaning to bgp.

down    Do not start the session when bgpd comes up but stay in IDLE.

dump (all|updates) (in|out) file [timeout]
        Do a peer specific MRT dump.  Peer specific dumps are limited to
        all and updates.  See also the dump section in GLOBAL
        CONFIGURATION.

enforce neighbor-as (yes|no)
        If set to yes, AS paths whose leftmost AS is not equal to the
        remote AS of the neighbor are rejected and a NOTIFICATION is sent
        back.  The default value for IBGP peers is no otherwise the de-
        fault is yes.

holdtime seconds
        Set the holdtime in seconds.  Inherited from the global configu-
        ration if not given.

holdtime min seconds
        Set the minimal acceptable holdtime.  Inherited from the global
        configuration if not given.

local-address address
        When bgp initiates the TCP connection to the neighbor system,
        it normally does not bind to a specific IP address.  If a local-
        address is given, bgp binds to this address first.

max-prefix number [restart number]
        Terminate the session after number prefixes have been received
        (no such limit is imposed by default).  If restart is specified,
        the session will be restarted after number minutes.

multihop hops
        Neighbors not in the same AS as the local bgp normally have
        to be directly connected to the local machine.  If this is not
        the case, the multihop statement defines the maximum hops the
        neighbor may be away.
```

```
     passive
             Do not attempt to actively open a TCP connection to the neighbor
             system.

     remote-as as-number
             Set the AS number of the remote system.

     route-reflector [address]
             Act as an RFC 2796 route-reflector for this neighbor.  An option-
             al cluster ID can be specified; otherwise the BGP ID will be
             used.

     set attribute ...
             Set the AS path attributes to some default per neighbor or group
             block:

                   set localpref 300

             See also the ATTRIBUTE SET section.  Set parameters are applied
             to the received prefixes; the only exceptions are prepend-self,
             nexthop no-modify and nexthop self.

     softreconfig (in|out) (yes|no)
             Turn soft reconfiguration on or off for the specified direction.
             If soft reconfiguration is turned on, filter changes will be ap-
             plied on configuration reloads.  If turned off, a BGP session
             needs to be cleared to apply the filter changes.  Enabling
             softreconfig in will raise the memory requirements of bgp be-
             cause the unmodified AS path attributes need to be stored as
             well.

     tcp md5sig password secret
     tcp md5sig key secret
             Enable TCP MD5 signatures per RFC 2385.  The shared secret can
             either be given as a password or hexadecimal key.

                   tcp md5sig password mekmidasdigoat
                   tcp md5sig key deadbeef

     ttl-security (yes|no)
             Enable or disable ttl-security.  When enabled, outgoing packets
             are sent using a TTL of 255 and a check is made against an incom-
             ing packet's TTL.  For directly connected peers, incoming packets
             are required to have a TTL of 255, ensuring they have not been
             routed.  For multihop peers, incoming packets are required to
             have a TTL of 256 minus multihop distance, ensuring they have not
             passed through more than the expected number of hops.  The de-
             fault is no.

Filter
     BGP has the ability to allow and deny UPDATES based on prefix or AS
     path attributes.  In addition, UPDATES may also be modified by filter
     rules.

     For each UPDATE processed by the filter, the filter rules are evaluated
     in sequential order, from first to last.  The last matching allow or deny
     rule decides what action is taken.

     The following actions can be used in the filter:

     allow     The UPDATE is passed.
     deny      The UPDATE is blocked.

     match     Apply the filter attribute set without influencing the filter
               decision.

PARAMETERS
     The rule parameters specify the UPDATES to which a rule applies.  An
     UPDATE always comes from, or goes to, one neighbor.  Most parameters are
     optional, but each can appear at most once per rule.  If a parameter is
     specified, the rule only applies to packets with matching attributes.

     as-type as-number
             This rule applies only to UPDATES where the AS path matches.  The
             as-number is matched against a part of the AS path specified by
             the as-type.  as-type is one of the following operators:

             AS           (any part)
             source-as    (rightmost AS number)
             transit-as   (all but the rightmost AS number)

             Multiple as-number entries for a given type or as-type as-number
             entries may also be specified, separated by commas or whitespace,
             if enclosed in curly brackets:

                   deny from any AS { 1, 2, 3 }
                   deny from any { AS 1, source-as 2, transit-as 3 }
                   deny from any { AS { 1, 2, 3 }, source-as 4, transit-as 5 }

     community as-number:local
     community name
             This rule applies only to UPDATES where the community path at-
             tribute is present and matches.  Communities are specified as as-
             number:local, where as-number is an AS number and local is a lo-
             cally significant number between zero and 65535.  Both as-number
             and local may be set to `*' to do wildcard matching.  Alterna-
             tively, well-known communities may be given by name instead and
             include NO_EXPORT, NO_ADVERTISE, NO_EXPORT_SUBCONFED, and
             NO_PEER.  Both as-number and local may be set to neighbor-as,
             which is expanded to the current neighbor remote AS number.

     (from|to) peer
             This rule applies only to UPDATES coming from, or going to, this
             particular neighbor.  This parameter must be specified.  peer is
             one of the following:

             any          Any neighbor will be matched.
             address      Neighbors with this address will be matched.
             group descr  Neighbors in this group will be matched.

             Multiple peer entries may also be specified, separated by commas
             or whitespace, if enclosed in curly brackets:

                   deny from { 128.251.16.1, 251.128.16.2, group hojo }

     prefix address/len
             This rule applies only to UPDATES for the specified prefix.

             Multiple address/len entries may be specified, separated by com-
             mas or whitespace, if enclosed in curly brackets:

                   deny from any prefix { 192.168.0.0/16, 10.0.0.0/8 }
             Multiple lists can also be specified, which is useful for macro
             expansion:

                   good="{ 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 }"
                   bad="{ 224.0.0.0/4, 240.0.0.0/4 }"
                   ugly="{ 127.0.0.1/8, 169.254.0.0/16 }"

                   deny from any prefix { $good $bad $ugly }

     prefixlen range
             This rule applies only to UPDATES for prefixes where the pre-
             fixlen matches.  Prefix length ranges are specified by using
             these operators:

                   =       (equal)
                   !=      (unequal)
                   <       (less than)
                   <=      (less than or equal)
                   >       (greater than)
                   >=      (greater than or equal)
                   -       (range including boundaries)
                   ><      (except range)

             >< and - are binary operators (they take two arguments).  For in-
             stance, to match all prefix lengths >= 8 and <= 12, and hence the
             CIDR netmasks 8, 9, 10, 11 and 12:

                   prefixlen 8-12

             Or, to match all prefix lengths < 8 or > 12, and hence the CIDR
             netmasks 0-7 and 13-32:

                   prefixlen 8><12

             prefixlen can be used together with prefix.

             This will match all prefixes in the 10.0.0.0/8 netblock with net-
             masks longer than 16:

                   prefix 10.0.0.0/8 prefixlen > 16

     quick   If an UPDATE matches a rule which has the quick option set, this
             rule is considered the last matching rule, and evaluation of sub-
             sequent rules is skipped.

     set attribute ...
             All matching rules can set the AS path attributes to some de-
             fault.  The set of every matching rule is applied, not only the
             last matching one.  See also the following section.

ATTRIBUTE SET
     AS path attributes can be modified with set.

     set can be used on network statements, in neighbor or group blocks, and
     on filter rules.  Attribute sets can be expressed as lists.

     The following attributes can be modified:

     community [delete] as-number:local
     community [delete] name
             Set or delete the COMMUNITIES AS path attribute.  Communities are
             specified as as-number:local, where as-number is an AS number and
```

```
            local is a locally-significant number between zero and 65535.
            Alternately, well-known communities may be specified by name:
            NO_EXPORT, NO_ADVERTISE, NO_EXPORT_SUBCONFED, or NO_PEER.

    localpref number
            Set the LOCAL_PREF AS path attribute.  If number starts with a
            plus or minus sign, LOCAL_PREF will be adjusted by adding or sub-
            tracting number; otherwise it will be set to number.

    med number
    metric number
            Set the MULTI_EXIT_DISC AS path attribute.  If number starts with
            a plus or minus sign, MULTI_EXIT_DISC will be adjusted by adding
            or subtracting number; otherwise it will be set to number.

    nexthop (address|blackhole|reject|self|no-modify)
            Set the NEXTHOP AS path attribute to a different nexthop address
            or use blackhole or reject routes.  If set to no-modify, the nex-
            thop attribute is not modified.  Unless set to self, the nexthop
            is left unmodified for IBGP sessions.  self forces the nexthop to
            be set to the local interface address.

                  set nexthop 192.168.0.1
                  set nexthop blackhole
                  set nexthop reject
                  set nexthop no-modify
                  set nexthop self

    prepend-neighbor number
            Prepend the neighbor's AS number times to the AS path.

    prepend-self number
            Prepend the local AS number times to the AS path.

    weight number
            The weight is used to tip prefixes with equally long AS paths in
            one or the other direction.  A prefix is weighed at a very late
            stage in the decision process.  If number starts with a plus or
            minus sign, the weight will be adjusted by adding or subtracting
            number; otherwise it will be set to number.  Weight is a local
            non-transitive attribute and a bgp specific extension.
```