Installing and Configuring BGPmon:
Quickstart Guide Version 1.1

This guide was tested on Ubuntu 11.04 and Fedora 14.0. Configuration for BGPmon is based on Cisco IOS. To see the list of available BGPmon commands, enter "?" for a collapsed list of commands. Enter "??" for an expanded list of commands. Command arguments can also be displayed by entering "?" after an available command. Command sets will vary depending on which mode the user is in.

The latest version of BGPmon can be downloaded from:
http://bgpmon.netsec.colostate.edu/index.php/download

A more comprehensive guide, the Administrator's Reference Manual, can be found in the BGPmon download package in 'bgpmon/doc/arm/'. The ARM can also be downloaded from:
http://bgpmon.netsec.colostate.edu/index.php/documentation.

1 Install BGPmon

```
> ./configure
> make
> make install
```

=> common solutions if above fails:
– Ubuntu: apt-get install libxml2-dev
– Fedora: yum install libxml2-devel

2 Launch BGPmon

```
> bgpmon -d -s
```

The -d option runs BGPmon in daemon mode; -s option logs BGPmon messages to /var/log/messages. For optional command line arguments, refer to ARM section 2.5.1.

3 Configure Command Line Access

The first priority when running BGPmon for the first time is to configure *privileged* access to the system. BGPmon is listening on the loopback address and port 50,000 for incoming connections. Use telnet to connect to the BGPmon server. After connecting to BGPmon, you will be prompted for a guest password. By default, the guest password is "BGPmon".

3.1 Enter guest mode

```
> telnet localhost 50000
Password:
```

Now, you are in *guest mode* that allows to view statistics, show routing tables, and generally view (but not change) configuration parameters. In order to change the configuration settings, switch to *privileged mode*.

3.2 Enter privileged mode

```
host> enable
enable password:
```

'BGPmon' is the default password to enter *privileged mode*.

From *privileged mode* you need to enter *configure mode* to gain access to all the configuration commands. To enter this mode type:

3.3 Enter configure mode

```
host# configure
host(config)#
```

3.4 Change guest mode and privileged mode passwords

```
host(config)# password [new password]
host(config)# enable password [new password]
```

Changes guest mode and privileged mode passwords, respectively.

3.5 Save changes

```
host(config)# exit
host# copy running-config startup-config
```

Ensures changes persist after a restart.
For BGPmon login recovery, refer to ARM section 3.1.2.

4 Configure Data Input

A BGPmon can receive data from three types of input: router, chain, and MRT collector. These can be used simultaneously.

4.1 Peer with router

=> Must be done in *configure* mode.

4.1.1 Add router

```
host(config)# router bgp [AS number]
host(config-router)# neigbor [IP address] remote as [Remote-AS-number]
host(config-router)# exit
host(config)# exit
host# copy running-config startup-config
```

This configuration enables BGP peering session with a router.
For configuration of parameters, refer to ARM sections 3.6.3 and 3.6.4.
For creation of peer-groups, refer to ARM section 3.6.2.

4.2 Setup a chain

A chain is a connection between BGPmons that allows one BGPmon to receive the XML output of another BGPmon.
=> Must be in configuration mode to configure chains.

4.2.1 Add or delete a chain

```
host(config)# chain [address] [port]
host(config)# no chain [address] [port]
host(config)# exit
host# copy running-config startup-config
```

Adds a chain, deletes a chain, and ensures changes persist, respectively.
For more chaining information, refer to ARM section 3.5.

4.3 Peer with MRT collector

Peering with an MRT collector only requires that the collector point at the BGPmon, in other words, send data to BGPmon. This is done via the MRT collector's interface. The collector must be included in the corresponding ACL; the default behavior is that all MRT collectors are allowed. The default MRT listener port is 7777. See the ARM section 3.4 for information about configuring ACLs.

5 Optional: Change Default Ports

By default, BGPmon sends BGP update messages on port 50001 and full BGP RIB tables on port 50002. The default admin login port is 50000, and the default MRT listener port is 7777. An admin can change these default values.

=> Must be in *config* mode

5.1 Change default data output ports

```
host(config)# client-listener update port [new-port]
host(config)# client-listener rib port [new-port]
host(config)# exit
host# copy running-config startup-config
```

5.2 Change default admin and MRT ports

```
host(config)# login-listener port [new-port]
host(config)# mrt-listener port [new-port]
host(config)# exit
host# copy running-config startup-config
```

6 Optional: Limit access to system

An administrator can limit access to the system via Access Control Lists (ACLs). These ACLs can be applied to clients, MRT collectors, the CLI, etc. Typical uses of ACLs limit access to subnets and/or single machines for remote access. The following demonstrates how to create a generic ACL. Note that these access lists are based on Cisco IOS Access Lists. Acls 'permitall' and 'denyall' are included as default acls.

6.1 Limit access via ACL

=> Must be in *config* mode

6.1.1 Create and Edit ACL

```
host(config)# acl [aclname]
Created ACL, now editing: [aclname]
host(config-acl)# permit [address] [subnet mask] [index num]
host(config-acl)# deny [address] [subnet mask] [index num]
host(config-acl)# show acl
```

Creates new acl if it doesn't exist, otherwise edits acl. Permit and deny as many machines and/or subnets as necessary.

6.1.2 Delete Rules and Commit Changes

```
host(config-acl)# no [index num]
host(config-acl)# exit
host(config)# exit
host# copy running-config startup-config
```

Deletes a rule from the acl by index number. For more acl commands, see the ARM command-list appendix.

6.1.3 Setting ACL

```
host# configure
host(config)# login-listener acl [login-acl]
host(config)# client-listener update acl [client-acl]
host(config)# client-listener rib acl [client-acl]
host(config)# mrt-listener acl [mrt-acl]
host(config)# exit
host# copy running-config startup-config
```

Sets admin acl, client update acl, client rib acl, and mrt acl, respectively.

7 Shutting Down BGPmon

Shutting down BGPmon can be done via the command-line interface. Open a telnet connection to BGPmon on the default admin port 50000. Enter enable mode, then enter the command "shutdown".

```
> telnet localhost 50000
Password:
host> enable
```

```
Password:
host# shutdown
```