

BIG BROTHER PROFESSIONAL EDITION

Network Architecture Summary

Big Brother is a simple system and network monitor which produces a web page containing a matrix of test results. Big Brother also has a modern looking sophisticated Flash display giving you a single pane of glass for monitored devices from multiple management servers. These test results are shown as red, green, yellow, purple, clear or blue dots.

A live demo is available at <http://www.bb4.com>

1. Components

Big Brother uses a client/server model, and is comprised of the following parts:

BBDISPLAY: The Display Server which processes the status information and creates the BB web pages and Flash display. Note that a web server such as Apache, or, IIS is needed to view the display pages.

BBPAGER: The Paging Server which processes alerts and dispatches them to the correct people. Notifications can be sent out by e-mail, SMS text, alpha/numeric pages and/or SNMP trap.

BBNET: The Network Monitor testing routine. Most common network protocols are supported (http/ftp/pop3/etc). Simple text-based protocols can be easily added to the configuration and monitored for availability.

LSM: Local system monitors (bbclients) which collect local system information and send it to the BBDISPLAY and/or BBPAGER if there's an error.

2. Architecture

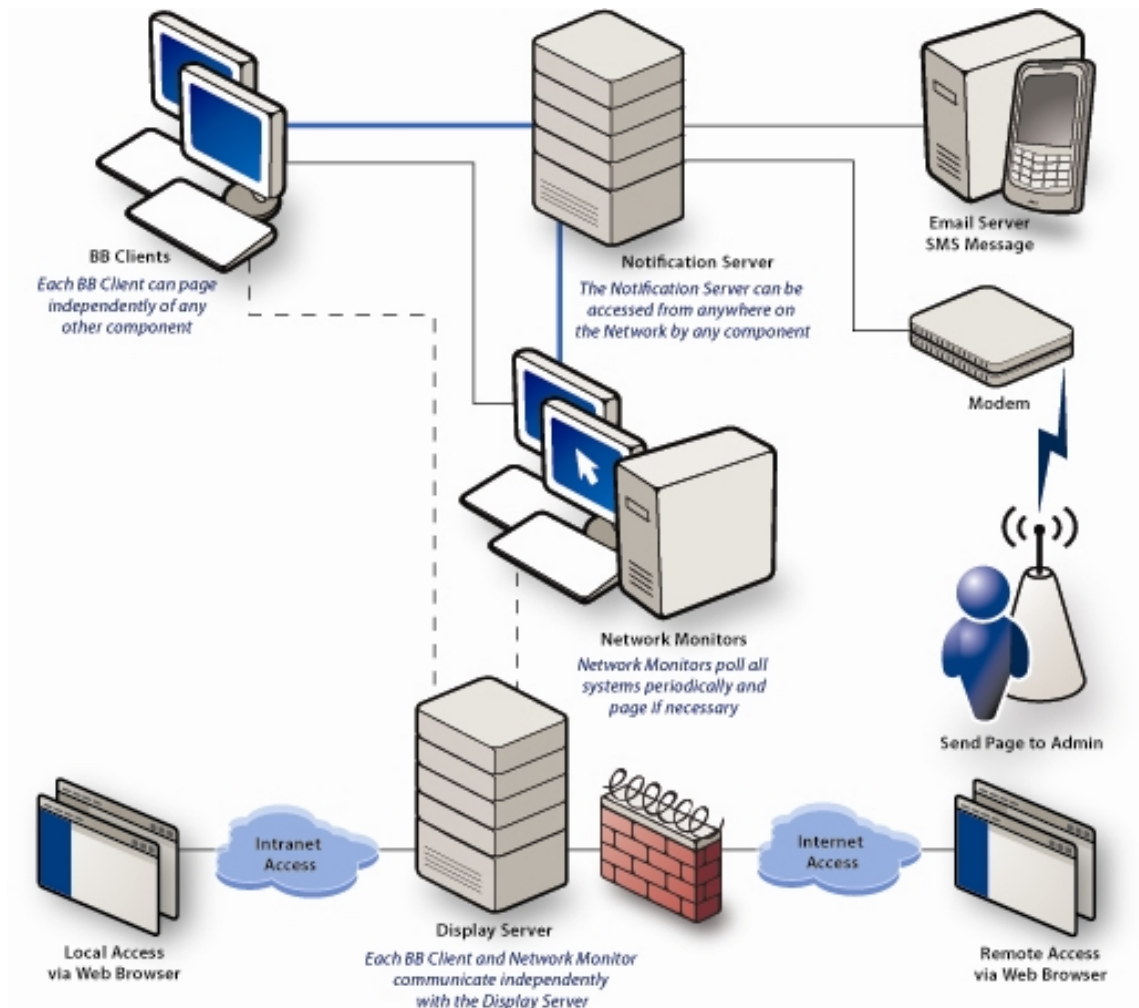
Communications: TCP/1984 (Configurable port).

BB communicates from client to server over TCP port 1984, which is registered with the IANA. The server accepts incoming client connections, uses them if valid, drops them if not, BB does not identify itself on connection or send an ACK of any sort to discourage hackers.

Architecture: Clients send their local system information to the BB servers (BBDISPLAY and BBPAGER) every 5 minutes (configurable). Redundancy can be achieved by having BB clients send status messages to multiple BBDISPLAYs and BBPAGERS without failover configuration.

The BBDISPLAYs themselves can be 'stacked' in such a way that the output from multiple BBDISPLAYs can be fed to a central BBDISPLAY allowing you cover an entire country, for example.

BBNET tests all listed services for all listed hosts every 5 minutes as well and sends the results to the BB servers. Note that by default BBNET is usually the same machine as the BBDISPLAY.



3. Protocol:

BB messages are simple, sent as text, and can be sent to the BBDISPLAY and BBPAGER using the 'bb' command. The format is:

```
bb 123.123.123.123 "type color machine.test data"
```

123.123.123.123: IP address of server
type: type of message – status, page, etc
machine.test: machine name, and test column
data: usually the date, plus the output from the test

Sample:

```
bb 123.123.213.123 "status red bobo.disk 12:00 pm disk full"
```

Status messages that are sent across the wire can be encrypted. Big Brother encryption uses triple DES and shared secrets to enhance security.

Status messages are time stamped with an expiration date that lets the management server know when a report is no longer valid, which is usually an indication of a more serious problem.

4. Sizing and Configuration:

We recommend having at most, 500 monitored devices per Big Brother management server.

In general, BB is quite light, system requirements are minimal and most recent operating systems should have no trouble supporting BB out of the box.

Most configurations exist on the management server. Monitored devices, network tests, notification rules, security codes and more are setup on the BB server. Client side thresholds can be managed centrally from the BBDISPLAY, or, from a configuration editor.

5. Complex network support:

Big Brother can handle segmented and firewalled networks using the BBRELAY directive, which allows you to route BB messages from one internal BBDISPLAY to another, external BBDISPLAY.

In addition we support point-to-point 128 bit encryption through the use of shared keys.

6. Customization and custom tests

Possibly the greatest strength of Big Brother is its ability to support custom tests in a quick and simple way. These tests can be written in any language.

If you can determine a status of red, yellow, or green, then it can be a BB test. In fact tests you already have running can be easily modified by simply adding the bb status command (described above) at the end of your test.

The BB display automatically shows new tests when they arrive.

The community site hosts 1000+ scripts, extensions, plug-ins and documentation to enhance and expand the monitor capabilities of Big Brother. The community site is located at: <http://www.bb4.com/community>, or, <http://www.deadcat.net>

If you have any questions please send us an email at bbsales@quest.com or call us at 949-754-8000.