



CHAPTER 6

Configuring the Syslog Utility to Receive BAC Alerts

This chapter describes how to configure the syslog utility after you install the Cisco Broadband Access Center (BAC). You can configure the syslog file on any BAC component server to receive alerts and debugging information from the system.



Note Configuring the syslog file is an optional task.

Syslog is a client-server protocol that manages the logging of information on UNIX. BAC generates alerts through the Solaris syslog service. BAC syslog alerts are not a logging service; they notify that a problem exists, but do not necessarily define the specific cause of the problem. The information related to the problem resides in the appropriate BAC log files (*rdulog* and *dpe.log*). If you choose to configure the syslog file, syslog alerts are directed to a separate log file.

For more information on error messages and alerts, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.

To configure the syslog utility on the RDU:

Step 1 Log in as *root* on the RDU server.

Step 2 At the command line, create the log file.

For example:

```
# touch /var/log/bac.log
```

Step 3 Open the */etc/syslog.conf* file with a text editor, such as *vi*.

Step 4 Add the following lines to the */etc/syslog.conf* file:

```
local6.alert      /var/log/bac.log
local6.info       /var/log/bac.log
```



Note You must insert one or more tabs between the *local6:info* and */var/log/bac.log* information.

Step 5 Save and close the */etc/syslog.conf* file.

Step 6 To force the syslog utility to take the new configuration, at the command line, enter:

```
# ps -ef | grep syslogd
root      217   1   0   Nov 26   ?   0:00   /usr/sbin/syslogd
```

```
kill -HUP 217
```



Note The process ID (PID) in this example is 217, but may change when you run `ps -ef | grep syslogd`. Use the correct output from that command as the input to `kill -HUP`.

Syslog is now ready to receive alerts from BAC.
