CHAPTER 4

Post-Installation Activities

This chapter describes the tasks that you perform after installing Cisco Broadband Access Center (BAC):

Licensing BAC

This BAC release enables licensing using a service file. These licenses allow you to provision a set number of services using BAC. Each service translates to three IP addresses provisioned in the system; thus, a 10,000 service license equates to 30,000 IP addresses. The license file that you receive will contain the number of IP addresses that are licensed, not the number of services that you purchased.

Caution Do not edit your license file. Changing the data in any way invalidates the license file.

You still require separate licenses for the following BAC components:

- The DPE
- The KDC, if you configure your network to support voice technology

The DPE license is contained within the license file and licenses the DPE when you install the license file from the administrator user interface. The KDC license continues to be proprietary, as in previous BAC releases, and is licensed during BAC installation.

For details on how to obtain your license file, refer to the *Release Notes for Cisco Broadband Access Center 4.0*.

Installing Your License File

Before installing your license file, ensure that you back up your licenses in case you have to reinstall the BAC software.

To install your permanent or evaluation license:

Step 1 Once you receive your license file, save each file to the local system on which you intend to launch your web browser.

Step 2 Launch your web browser on that system.

Step 3 Enter the administrator's location using this syntax:

`http://machine_name:port_number/`

- *machine_name*—Identifies the computer on which the RDU is running.

  Note To access the administrator user interface via HTTP over SSL, also known as HTTPS, enter: `https://machine_name:port_number/`

- *port_number*—Identifies the computer port on which the server side of the administrator application runs. The default port number is:
  - 8100 for HTTP over TCP
  - 8443 for HTTP over SSL

The main login page appears.

Step 4 Enter the default username (**admin**) and password (**changeme**).

Note If you are logging in for the first time, the Change Password screen appears. Enter a new password and confirm it.

Step 5 Click **Login**.

The Main Menu page appears.

Step 6 Click the license link at the top of the Main Menu page, or choose **Configuration > License Keys**.

The Manage License Keys page appears.

Step 7 In the License File field, enter the complete path to the location of the license file on your local system. Remember to include the name of the license file while specifying the pathname.

Or, click **Browse** and navigate to the license file.

Step 8 Click **Add/Upgrade**.

The details regarding the number of services and the DPEs that you are licensed to use appear.

Installing Your KDC License

Obtain a KDC license from your Cisco representative and then install it in the correct directory.

To install the KDC license file (*backkdc.license*):

Step 1 Obtain your license file from your Cisco representative.

Step 2 Log in to the BAC host as root.

Step 3 Change to the *BPR_HOME/kdc* directory.

Step 4 Copy the license file to this *BPR_HOME/kdc* directory.

Caution Be careful not to copy the license file as an ASCII file. The file contains binary data susceptible to unwanted modification during an ASCII transfer.

Do not copy KDC license files between operating systems because the transfer process may damage the file.

Step 5 To restart the KDC server and make the changes take effect, run the **bprAgent restart kdc** command from the */etc/init.d* directory.

Enabling a Network Registrar Spoofing DNS Server

A spoofing DNS server redirects all DNS requests to the same IP address. You can enable spoofing to enforce a self-provisioning flow for a new subscriber.

For example, assume that a DNS host is dns.example.com, and has an IP address of 10.10.10.5. Assume also that the web server with the self-provisioning flow is 10.10.10.6.

On the DNS server, set the following parameters in Cisco Network Registrar:

```
nrcmd> zone . delete
nrcmd> zone . create primary dns.example.com postmaster.dns.example.com
nrcmd> zone . addrr * a 10.10.10.6
nrcmd> save
nrcmd> dns reload
```

When DNS reloads, the changes take effect.

On the DHCP server, set the following parameters in Network Registrar:

```
nrcmd> policy unprovisioned setoption domain-name-servers 10.10.10.5
nrcmd> policy unprovisioned setoption domain-name example.com
nrcmd> save
nrcmd> dhcp reload
```

Configuring the Syslog Utility to Receive Alerts from 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.

BAC generates alerts through the Solaris syslog service. Syslog is a client-server protocol that manages the logging of information on UNIX. 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. This information might reside in the appropriate BAC log files (*rdu.log* and *dpe.log*). If you choose to configure the syslog file, these alerts are directed to a separate log file.

For more information on error messages and alerts, refer to the *Cisco Broadband Access Center Administrator Guide 4.0*.

To configure the syslog utility on the Network Registrar extension points and the RDU server:

Step 1 Log in, as *root,* on the Network Registrar 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 this line to the */etc/syslog.conf* file:

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

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

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

Step 6 To force the syslog utility to accept the new configuration, enter:

```
# ps -ef  | grep syslogd
    root    217    1    0    Jun 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.