The HP diagnostic commands are tools that you can use to gather information about HP devices. The diagnostic commands start with **de**, **debug**, **mm**, **phy**, and **ptrace**.

- **de** Displays information about CPU buffer allocations.
- **debug** Reports debugging information that you can use to resolve configuration problems.
- **mm** Displays the contents of a specified address on every module. (Available on Chassis devices only)
- **phy** Displays information about PHY (hardware) registers for a specified port.
- **ptrace** Displays information on the console when a specified kind of packet is transmitted or received.

In addition, the **show ip bgp debug** command reports information about resource allocation and errors in a BGP configuration.

These commands are available in Privileged EXEC mode on the Command Line Interface (CLI) only. You cannot use them in the device's Web management interface. For complete syntax information for the diagnostic commands, see the next chapter, “HP Diagnostic Command Reference” on page 3-1.

Many of the diagnostic commands are meant to be used in conjunction with calls to HP technical support. If you report a problem, the support engineer may ask you to execute one or more of the diagnostic commands described in this guide. Some of the diagnostic commands report information about internal hardware settings and registers that is relevant primarily to HP engineering staff. Consequently, this information is not described in detail here.

The following table lists some of the tasks you can perform using the diagnostic commands:

<table>
<thead>
<tr>
<th>Task</th>
<th>Relevant Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing packets</td>
<td>ptrace</td>
</tr>
</tbody>
</table>
| Displaying AppleTalk information | debug appletalk  
                            | ptrace appletalk               |
| Displaying BGP information | debug ip bgp  
                            | show ip bgp debug             |
| Displaying IPv6 information | debug ipv6     |
| Displaying OSPF packet information | debug ip ospf packet  |
### Using an ACL to Filter Debug Output

You can use an ACL to filter output from `debug` commands. For example, you can set up an ACL that permits packets from an IP address, then apply that ACL to a `debug` command. When you start the `debug` command, only messages related to that IP address are displayed in the output for that command.

The following example limits output from the `debug ip tcp packet` command to only messages related to incoming packets from `10.10.10.10`.

First, set up an ACL to permit packets from host `10.10.10.10`. For example:

```
ProCurveRS(config)# access-list 100 permit ip host 10.10.10.10 any
```

Then apply this ACL to the `debug ip tcp` command. You can specify no more than one ACL per protocol.

```
ProCurveRS# debug ip tcp acl 100
```

**Syntax:** `debug ip <protocol> acl <acl-id>

Then enter the `debug ip tcp packet` command to start generating debug output.

```
ProCurveRS# debug ip tcp packet
```

**Syntax:** `[no] debug ip tcp packet

Only messages related to packets inbound from `10.10.10.10` are displayed in the output for the `debug ip tcp packet` command. To display messages related to outbound packets sent to `10.10.10.10`, add another entry to the ACL, specifying `10.10.10.10` as the destination host. For example:

```
ProCurveRS(config)# access-list 100 permit ip any host 10.10.10.10
```

**The show debug** command displays ACLs applied to debug commands. For example:

```
ProCurveRS# show debug
Debug message destination: Console
TCP:
    TCP: packet debugging is on
    TCP: Display is bound to ACL 100
```

**Syntax:** `show debug`