In a Denial of Service (DoS) attack, a Routing Switch is flooded with useless packets, hindering normal operation. HP devices include measures for defending against two types of DoS attacks: Smurf attacks and TCP SYN attacks.

Protecting Against Smurf Attacks

A Smurf attack is a kind of DoS attack where an attacker causes a victim to be flooded with ICMP echo (Ping) replies sent from another network. Figure 7.1 illustrates how a Smurf attack works.

Figure 7.1 How a Smurf attack floods a victim with ICMP replies

1. The attacker sends ICMP echo requests to the broadcast address on an intermediary's network, spoofing the victim's IP address as the source.

2. If the intermediary has directed broadcast forwarding enabled, ICMP echo requests are broadcast to hosts on the intermediary's network.

3. The hosts on the intermediary's network send replies to the victim, inundating the victim with ICMP packets.

The attacker sends an ICMP echo request packet to the broadcast address of an intermediary network. The ICMP echo request packet contains the spoofed address of a victim network as its source. When the ICMP echo request reaches the intermediary network, it is converted to a Layer 2 broadcast and sent to the hosts on the intermediary network. The hosts on the intermediary network then send ICMP replies to the victim network.
For each ICMP echo request packet sent by the attacker, a number of ICMP replies equal to the number of hosts on the intermediary network are sent to the victim. If the attacker generates a large volume of ICMP echo request packets, and the intermediary network contains a large number of hosts, the victim can be overwhelmed with ICMP replies.

Avoiding Being an Intermediary in a Smurf Attack

A Smurf attack relies on the intermediary to broadcast ICMP echo request packets to hosts on a target subnet. When the ICMP echo request packet arrives at the target subnet, it is converted to a Layer 2 broadcast and sent to the connected hosts. This conversion takes place only when directed broadcast forwarding is enabled on the device.

To avoid being an intermediary in a Smurf attack, make sure forwarding of directed broadcasts is disabled on the HP device. Starting with release 06.0.00, directed broadcast forwarding is disabled by default. In releases prior to 06.0.00, directed broadcast forwarding is enabled by default. To disable directed broadcast forwarding, do one of the following:

**USING THE CLI**

ProCurveRS(config)# no ip directed-broadcast

**Syntax:** [no] ip directed-broadcast

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the **General** link to display the IP configuration panel.
5. Select Disable next to Directed Broadcast Forward.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the **Save** link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Avoiding Being a Victim in a Smurf Attack

You can configure the HP device to drop ICMP packets when excessive numbers are encountered, as is the case when the device is the victim of a Smurf attack. You can set threshold values for ICMP packets that are targeted or passing through an interface, and drop them when the thresholds are exceeded.

For example, to set threshold values for ICMP packets targeted, enter the following command in CONFIG mode:

```
ProCurveRS(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

To set threshold values for ICMP packets received on interface 3/11:

```
ProCurveRS(config)# int e 3/11
ProCurveRS(config-if-e100-3/11)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

**Syntax:** ip icmp burst-normal <value> burst-max <value> lockup <seconds>

The **burst-normal** value can be from 1 – 100000.

The **burst-max** value can be from 1 – 100000.

The **lockup** value can be from 1 – 10000.

The number of incoming ICMP packets per second are measured and compared to the threshold values as follows:

- If the number of ICMP packets exceeds the **burst-normal** value, the excess ICMP packets are dropped.
• If the number of ICMP packets exceeds the **burst-max** value, all ICMP packets are dropped for the number of seconds specified by the **lockup** value. When the lockup period expires, the packet counter is reset and measurement is restarted.

In the example above, if the number of ICMP packets received per second exceeds 5,000, the excess packets are dropped. If the number of ICMP packets received per second exceeds 10,000, the device drops all ICMP packets for the next 300 seconds (five minutes).

### Protecting Against TCP SYN Attacks

**TCP SYN attacks** exploit the process of how TCP connections are established in order to disrupt normal traffic flow. When a TCP connection starts, the connecting host first sends a TCP SYN packet to the destination host. The destination host responds with a SYN ACK packet, and the connecting host sends back an ACK packet. This process, known as a “TCP three-way handshake”, establishes the TCP connection.

While waiting for the connecting host to send an ACK packet, the destination host keeps track of the as-yet incomplete TCP connection in a connection queue. When the ACK packet is received, information about the connection is removed from the connection queue. Usually there is not much time between the destination host sending a SYN ACK packet and the source host sending an ACK packet, so the connection queue clears quickly.

In a TCP SYN attack, an attacker floods a host with TCP SYN packets that have random source IP addresses. For each of these TCP SYN packets, the destination host responds with a SYN ACK packet and adds information to the connection queue. However, since the source host does not exist, no ACK packet is sent back to the destination host, and an entry remains in the connection queue until it ages out (after around a minute). If the attacker sends enough TCP SYN packets, the connection queue can fill up, and service can be denied to legitimate TCP connections.

To protect against TCP SYN attacks, you can configure the HP device to drop TCP SYN packets when excessive numbers are encountered. You can set threshold values for TCP SYN packets that are targeted or passing through an interface, and drop them when the thresholds are exceeded.

For example, to set threshold values for TCP SYN packets targeted, enter the following command in CONFIG mode:

```bash
ProCurveRS(config)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

To set threshold values for TCP SYN packets received on interface 3/11:

```bash
ProCurveRS(config)# int e 3/11
ProCurveRS(config-if-e100-3/11)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

**Syntax:** `ip tcp burst-normal <value> burst-max <value> lockup <seconds>`

The **burst-normal** value can be from 1 – 100000.

The **burst-max** value can be from 1 – 100000.

The **lockup** value can be from 1 – 10000.

**NOTE:** The `ip tcp burst-normal` command is available at the global CONFIG level and.

The number of incoming TCP SYN packets per second are measured and compared to the threshold values as follows:

• If the number of TCP SYN packets exceeds the **burst-normal** value, the excess TCP SYN packets are dropped.

• If the number of TCP SYN packets exceeds the **burst-max** value, all TCP SYN packets are dropped for the number of seconds specified by the **lockup** value. When the lockup period expires, the packet counter is reset and measurement is restarted.

In the example above, if the number of TCP SYN packets received per second exceeds 10, the excess packets are dropped. If the number of TCP SYN packets received per second exceeds 100, the device drops all TCP SYN packets for the next 300 seconds (five minutes).
TCP Security Enhancement in Release 07.6.06

Software releases 07.6.06 and later provide a TCP security enhancement that improves upon the handling of TCP inbound segments. This enhancement eliminates or minimizes the possibility of a TCP reset attack, in which a perpetrator attempts to prematurely terminate an active TCP session, and a data injection attack, wherein an attacker injects or manipulates data in a TCP connection.

In both cases, the attack is blind, meaning the perpetrator does not have visibility into the content of the data stream between two devices, but blindly injects traffic. Also, the attacker does not see the direct effect, the continuing communications between the devices and the impact of the injected packet, but may see the indirect impact of a terminated or corrupted session.

The TCP security enhancement prevents and protects against the following three types of attacks:

- Blind TCP reset attack using the reset (RST) bit.
- Blind TCP reset attack using the synchronization (SYN) bit.
- Blind TCP packet injection attack.

The TCP security enhancement is automatically enabled in software releases 07.6.06 and later. If necessary, you can disable this feature. See “Disabling the TCP Security Enhancement” on page 7-5.

Protecting Against a Blind TCP Reset Attack Using the RST Bit

In a blind TCP reset attack using the RST bit, a perpetrator attempts to guess the RST segments in order to prematurely terminate an active TCP session.

Software releases prior to 07.6.06 apply the following rules to the RST bit when receiving TCP segments:

- If the RST bit is set and the sequence number is outside the expected window, the HP device silently drops the segment.
- If the RST bit is set and the sequence number is within the acceptable range, the HP device resets the connection.

To prevent a user from using the RST bit to reset a TCP connection, in software releases 07.6.06 and later, the RST bit is subject to the following rules when receiving TCP segments:

- If the RST bit is set and the sequence number is outside the expected window, the HP device silently drops the segment.
- If the RST bit is exactly the next expected sequence number, the HP device resets the connection.
- If the RST bit is set and the sequence number does not exactly match the next expected sequence value, but is within the acceptable window, the HP device sends an acknowledgement.

This TCP security enhancement is enabled by default in software releases 07.6.06 and later. To disable it, see “Disabling the TCP Security Enhancement” on page 7-5.

Protecting Against a Blind TCP Reset Attack Using the SYN Bit

In a blind TCP reset attack, a perpetrator attempts to guess the SYN bits to prematurely terminate an active TCP session.

Software releases prior to 07.6.06 apply the following rules to the SYN bit when receiving TCP segments:

- If the SYN bit is set and the sequence number is outside the expected window, the HP device sends an ACK back to the sender.
- If the SYN bit is set and the sequence number is acceptable, the HP device sends a RST segment to the peer.

To prevent a user from using the SYN bit to tear down a TCP connection, in software releases 07.6.06 and later, the SYN bit is subject to the following rules when receiving TCP segments:

- If the SYN bit is set and the sequence number is outside the expected window, the HP device sends an acknowledgement (ACK) back to the peer.
- If the SYN bit is set and the sequence number is an exact match to the next expected sequence, the HP...
device sends an ACK segment to the peer. Before sending the ACK segment, the software subtracts one from the value being acknowledged.

- If the SYN bit is set and the sequence number is acceptable, the HP device sends an acknowledgement (ACK) segment to the peer.

In software releases 07.6.06 and later, the TCP security enhancement is enabled by default. To disable it, see “Disabling the TCP Security Enhancement” on page 7-5.

**Protecting Against a Blind Injection Attack**

In a blind TCP injection attack, a perpetrator tries to inject or manipulate data in a TCP connection.

To reduce the chances of a blind injection attack, software releases 07.6.06 and later perform an additional check on all incoming TCP segments.

This TCP security enhancement is enabled by default. To disable it, see “Disabling the TCP Security Enhancement” on page 7-5.

**Disabling the TCP Security Enhancement**

The TCP security enhancement is automatically enabled in software releases 07.6.06 and later. If necessary, you can disable this feature. When you disable this feature, the HP device reverts to the original behavior (i.e., processes TCP segments as in releases prior to 07.6.06).

To disable the TCP security enhancement, enter the following command at the Global CONFIG level of the CLI:

```
ProCurveRS(config)# no ip tcp tcp-security
```

To re-enable the TCP security enhancement once it has been enabled, enter the following command:

```
ProCurveRS(config)# ip tcp tcp-security
```

**Syntax:** `[no] ip tcp tcp-security`

**Displaying Statistics about Packets Dropped Because of DoS Attacks**

To display information about ICMP and TCP SYN packets dropped because burst thresholds were exceeded:

```
ProCurveRS(config)# show statistics dos-attack
```

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:** `show statistics dos-attack`

To clear statistics about ICMP and TCP SYN packets dropped because burst thresholds were exceeded:

```
ProCurveRS(config)# clear statistics dos-attack
```

**Syntax:** `clear statistics dos-attack`