



Specials Documentation

“Fault Finder Thresholds”

HP switches feature automatic fault detection, which helps protect against network loops and defective equipment. The fault detection sensitivity setting determines the types of alerts reported to the Alert Log based on their level of severity or sensitivity. The sensitivity levels are:

- **High Sensitivity.** This policy directs the switch to send all alerts to the Alert Log. This setting is most effective on networks that have none or few problems.
- **Medium Sensitivity.** This policy directs the switch to send alerts related to network problems to the Alert Log. If you want to be notified of problems which cause a noticeable slowdown on the network, use this setting.
- **Low Sensitivity.** This policy directs the switch to send only the most severe alerts to the Alert Log. This policy is most effective on a network where there are normally a lot of problems and you want to be informed of only the most severe ones.
- **Disabled.** Disables the Alert Log and transmission of alerts (traps) to the management server (in cases where a network management tool such as ProCurve Manager is in use). Use this option when you don't want to use the Alert Log.

Enabling Fault Finder Using the CLI

Enter this CLI command to enable fault detection.

Syntax: [no] fault-finder [fault] [sensitivity <low | medium | high>] [action <warn | warn-and-disable>]

Enables or disables Fault Finder and sets sensitivity.

*When the **warn-and-disable** action option is configured, Fault Finder may also shut down a bad port in addition to sending an alert to the Alert Log.*

*Default setting: **fault-finder sensitivity medium action warn***

[fault]: *Supported values are:*

- **all:** All fault types
- **bad-driver:** Too many undersized/giant packets
- **bad-transceiver:** Excessive jabbering
- **bad-cable:** Excessive CRC/alignment errors
- **too-long-cable:** Excessive late collisions
- **over-bandwidth:** High collision or drop rate
- **broadcast-storm:** Excessive broadcasts
- **duplex-mismatch-HDx:** Duplex mismatch. Reconfigure to Full Duplex
- **duplex-mismatch-FDx:** Duplex mismatch. Reconfigure port to Auto
- **link-flap:** Rapid detection of link faults and recoveries
- **loss-of-link:** Link loss detected. (Sensitivity not applicable)

Example Settings

To set Fault Finder with a **high** sensitivity to issue a warning and then disable a port on which there is a high collision or drop rate, you could configure these options:

```
HPswitch(config)# fault-finder over-bandwidth sensitivity high action  
warn-and-disable
```

To set Fault Finder with a **medium** sensitivity to issue a warning about excessive CRC or alignment errors on a port, you could configure these options:

```
HPswitch(config)# fault-finder bad-cable sensitivity medium action warn
```

To set Fault Finder with a **low** sensitivity to issue a warning about rapid detection of link faults, you could configure these options:

```
HPswitch(config)# fault-finder link-flap sensitivity low action warn
```

To **disable** Fault Finder, enter this command:

```
HPswitch(config)# no fault-finder all
```

Table 1. Table of Fault Finder Sensitivities for Supported Conditions

Condition Triggering Fault Finder	Sensitivities			Units (in Packets)	Time Period	Fault Finder Reacts:
	High	Medium	Low			
Bad driver — Too many under-sized packets or too many giant packets	6	21	36	1/10,000 Incoming	20 secs	If (undersized/total) >= (sensitivity/10,000) Or If (giant/total) >= (sensitivity/10,000)
Bad transceiver — Excessive jabbering -Jabbers: (Jabbers are packets longer than the MTU) -Fragments: (packets shorter than they should be)	6 5	21 10	36 14	1/10,000 Incoming One Fragments	20 secs 20 secs	If (jabbers/total) >= (sensitivity/10,000) Or If fragment count in the last 20 seconds >= sensitivity
Bad cable — Excessive CRC/alignment errors	6	21	36	1/10,000 Incoming	20 secs	If (CRC and alignment errors/total) >= (sensitivity/10,000)
Too Long Cable — Excessive late collisions (a late collision error occurs after the first 512 bit times)	6	21	36	1/10,000 Outgoing	20 secs	If (late collisions/total) >= (sensitivity/10,000)
Over bandwidth -High collision rate -High drop rate	6 65	21 257	36 449	1/10,000 Outgoing One Packet	5 mins 5 mins	If (excessive collisions/total) >= (sensitivity/10,000) The count of dropped packets >= sensitivity during the last 5 minutes.
Broadcast storm — Excessive broadcasts	2750	9200	15600	One Broadcast Packet	1 sec	If the average per second of broadcast packets in the last 20 seconds >= sensitivity
Duplex mismatch HDx	6	21	36	1/10,000 Outgoing	20 sec	If (late collisions/total) >= (sensitivity/10,000)
Duplex mismatch FDx	6	21	36	1/10,000 Incoming	20 sec	If (CRC and alignment errors/total) >= (sensitivity/10,000)
Link flap — Excessive transitions between link-up and link-down states.	4	7	11	One Transitions	10 secs	If the Transition count in the last 10s >= sensitivity.

Example of Sensitivity Calculation

If a sensitivity is set to High, and a bad cable is causing 15 CRC errors out of a total of 3500 packets transmitted in a 20 second period:

1. CRC errors/total must be \geq (sensitivity/10,000) to trigger an alert.
2. CRC errors/total = $15/3500 = .00043$
3. Sensitivity/10,000 = $6/10,000 = .0006$
4. $.00043$ is not greater than or equal to $.0006$, so an alert is not triggered.