Understanding Storm Control on EX Series Switches

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and drop broadcast and unknown unicast packets when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading the LAN. Alternatively, you can configure the switch to shut down interfaces (see action-shutdown or temporarily disable interfaces (see port-error-disable) when the storm control level is exceeded.

By default, storm control is enabled on all switch interfaces at a level of 50 percent of the combined broadcast and unknown unicast streams. You can change the storm control level either by configuring it as a bandwidth value for the combined broadcast and unknown unicast traffic streams or by configuring it as a percentage of the combined broadcast and unknown unicast streams.

NOTE: The level configuration statement, which allows you to configure the storm control level as a percentage of the combined broadcast and unknown unicast streams, has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use and replace it with the bandwidth statement, which allows you to configure the storm control level as a bandwidth value for the combined broadcast and unknown unicast traffic streams.

Broadcast, multicast, and unicast packets are part of normal LAN operation, so to recognize a storm, you must be able to identify when traffic has reached a level that is abnormal for your LAN. Suspect a storm when operations begin timing out and network response times slow down. As more packets flood the LAN, network users might be unable to access servers or e-mail.

Monitor the percentage of broadcast and unknown unicast traffic in the LAN when it is operating normally. This data can then be used as a benchmark to determine when traffic levels are too high. You can then configure storm control to set the level at which you want to drop broadcast and unknown unicast traffic.

Related Topics

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)

Published: 2009-07-28