



Technology Brief:

Syslog Centralized Logging

What it Means to You:

- Centralized logging improves network management and records security
- Supports regulatory compliance

How Spectracom Supports Syslog (in the case of NetClock):

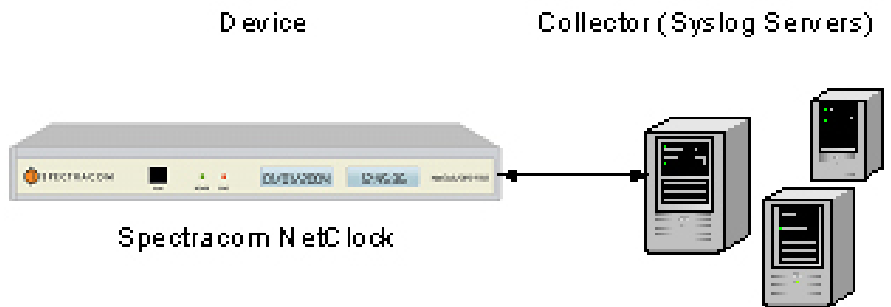
- NetClock is the Syslog "device"
- Syslog servers are the "collectors"
- NetClock can send messages to five Syslog servers to support world-wide network monitoring
- NetClock supports RFC 3164 – the BSD Syslog Protocol
- NetClock uses UDP, Port 514

What Can Administrators Do?

- Direct messages to different Syslog servers by internal log type
- Assign facility codes and severity levels to each scenario

Introduction

Spectracom's products provide critical timing services to various networking devices. They also support external logging to Syslog servers, a common centralized collector for error messages that is preferred by many network administrators.



Why Use Syslog?

Local logs are extremely useful in monitoring and troubleshooting timing issues in the enterprise network. (See the Tech Brief on Local Logging.) "Syslog" is an industry convention for collecting these logs or messages from network devices such as Spectracom products. Syslog stores this information on centralized Syslog servers. This produces tangible benefits:

- The network administrator may use Perl scripts or other utilities to monitor for specific patterns in the incoming log messages, such as evidence of multiple, denied authentication accesses. This practice provides real-time monitoring of network conditions.
- If a user edits or deletes the local logs on a network device, the administrator may review the protected logs on the Syslog server, which typically operates under higher security.

Applicable Products

- NetClock 9200 and 9300 Series
- SecureSync