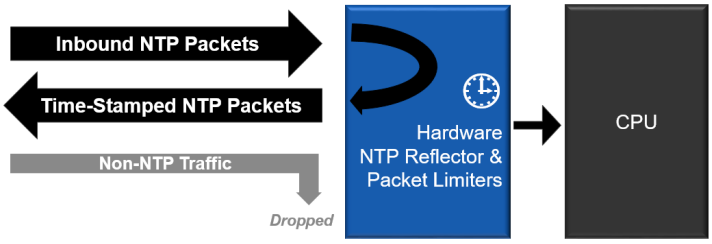
Security-Hardened NTP Reflector and Packet Limiting/Monitoring for TimeProvider 4100

TimeProvider 4100 implements real-time, hardware-based network packet processing in tandem with accurate hardware-based NTP timestamping, general packet limiting, and alarming. The intent is to protect the TimeProvider 4100 CPU from excessive network traffic denial of service (DoS) attacks, and, in the process, provide extremely high-bandwidth, high-accuracy NTP operations.



Microsemi's Unique NTP Reflector Technology

The NTP Reflector is a real-time, hardware-based NTP packet identification and timestamping engine. The high-capacity packet processor uses the exceptionally accurate TimeProvider 4100 clock to deliver the best possible NTP time stamps. At line speed, NTP client packets are identified, the precise and accurate T2 and T3 time stamps are added, and the packet is returned to the requesting NTP client. Because all operations are in hardware operating at 1 GbE line speed, the NTP packet capacity is in excess of 20,000 NTP packets per second. Currently, the NTP Reflector is configurable on one user-selectable port between ports 2 and 4–8.

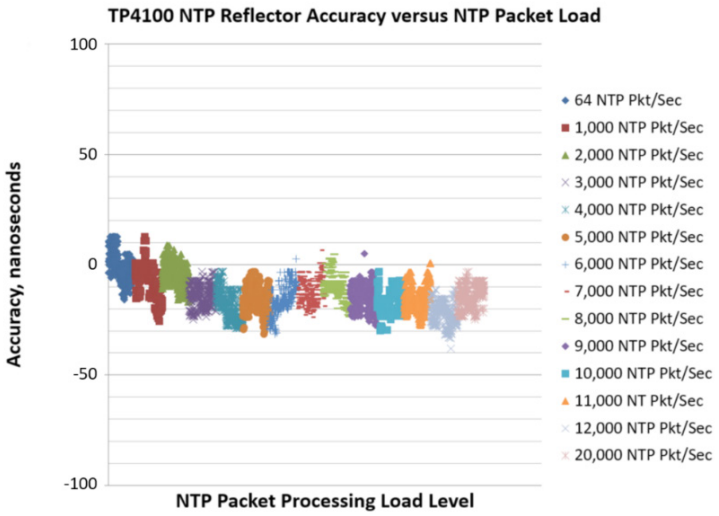
Advantages of NTP Reflector over NTP Daemon

The NTP Reflector supports the most common NTP mode 3 client requests for time. The NTP daemon, available in any other product, runs on the embedded CPU NTP server. The NTP daemon is UDP/IP and is by nature susceptible to DoS attacks as it does not require TCP/IP connection. The security-hardening of the line-speed NTP Reflector is such that in the event of an NTP DoS attack, the excessive NTP packets do not reach the CPU and compromise the server operation. Instead, all NTP packets are responded to, and if the NTP load is in excess of what is expected, an SNMP trap is sent notifying the user of the excess load.

NTP Reflector Performance vs. NTP Daemon Performance

It is important to understand the behavior of the hardware-based NTP Reflector versus the general and much more common software-based NTP daemon. Almost all network time servers use software timestamping. This means the NTP daemon requests time stamps from the supporting underlying hardware and the time packet exchanges transit up and down the operating system stack. These internal packet exchanges take time and are notorious for variable delays, especially when the CPU is busy. These delays are usually asymmetric (takes longer in one direction than another), varies from request to request, and the result is degraded timing accuracy of the time server overall. The NTP Reflector is not susceptible to these time accuracy reducing delays caused by CPU loading as all time stamping and NTP packet processing is performed 100% in hardware with virtually no asymmetric delays.

As shown in the following chart, the NTP packet load was incrementally increased (represented by color changes) while the performance of the NTP Reflector was measured with a near perfect NTP test instrument. The NTP Reflector performed deterministically with the time accuracy and precision of 15 nanoseconds RMS to UTC independent of NTP request load. There were no dropped packets as 100% of all NTP requests for time were responded to. This NTP timing accuracy and reliability is maintained all the way up to the full 1 GbE line speed at 20,000 NTP requests per second.



Security-Hardened NTP Reflector and Packet Limiting/Monitoring for TimeProvider 4100

TimeProvider 4100 CPU Protection

The TimeProvider 4100 CPU is optionally protected by two layers of hardware-based, network packet-limiting filters and extremely robust IP table rules.The first hardware layer is established on a per-LAN port basis. Unique rate limits can be set per port on the number of network packets allowed to pass towards the CPU. If the set limit is reached on any port, an SNMP trap alert is sent. Excessive packets beyond the set limits are dropped on a port-by-port basis. The next layer of protection is established in the hardware where the sum of all network packets across all LAN ports being directed to the CPU is not allowed to exceed a fixed Microsemi-defined limit that is not user-adjustable. Lastly, there are extremely robust software firewall configurations that severely limit the kinds of packets allowed to reach the CPU. Disallowed packet types are immediately dropped.

Hardware-Based DoS Protection

The advantage of this multilayer protection configuration is that it protects the TimeProvider 4100 server from many of the effects of a DoS attack. This does not mean that a service-affecting DoS attack cannot be directed at TimeProvider 4100 as excessive traffic from illegitimate clients can result in reduction of service to legitimate clients. What it does mean is that if unexpectedly high levels of packet loading of any kind occur beyond user-defined levels, a notification is sent and the excess packets are dropped. If the TimeProvider 4100 alarms, the user should examine if the traffic loads directed at the server are for legitimate reasons or for illegitimate ones. If the traffic is legitimate, then the user can choose to adjust the packet limit/alarm thresholds on the port(s). If the traffic is illegitimate, then the user can begin to track down the source of the excessive packet load. Through it all, the TimeProvider 4100 CPU remains protected from excessive packet loads that have been known to cause CPU faults on unprotected network devices.

NTP Reflector and NTP Packet Monitoring

The Ethernet port or ports selected to provide NTP Reflector services also are equipped with a user-defined alarm threshold. This threshold is for monitoring and notification purposes, not for NTP packet limiting. The NTP Reflector will always process all NTP time requests up to the full GbE-line speed of the Ethernet port. However, if the NTP client request load exceeds the user-set threshold, an SNMP trap is sent to notify that the load is beyond expected levels. NTP services from the NTP Reflector are limited only by the GbE throughput of the network link.

Peace-of-Mind NTP Operations

The primary intent of the security-hardened NTP Reflector and the associated packet limiting/alarming function is peace-of-mind NTP operations on the network. The phenomenal NTP capacity and time stamp accuracy of the NTP Reflector, along with its LAN port-hardening capability, are an ideal solution to provide very robust NTP time services to the network.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

MSCC-0104-AN-0101-1.00-0917