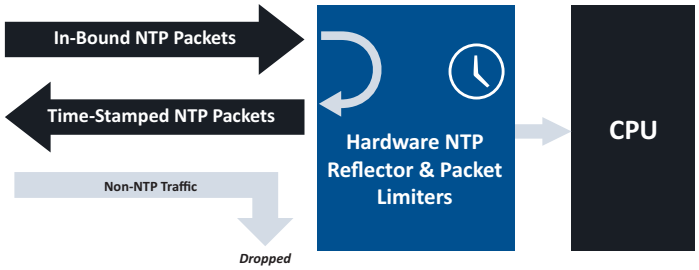
Security-Hardened NTP Reflector and Packet Limiting/ Monitoring for SyncServer® Network Time server

Summary

The SyncServer® network time server 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 SyncServer CPU from excessive network traffic denial-of-service (DoS) attacks, and in the process, provide extremely high-bandwidth, high-accuracy NTP operations.



Unique Reflector Technology NTP

The NTP Reflector is a real-time, hardware-based NTP packet identification and timestamping engine. The high-capacity packet processor uses the exceptionally accurate S600 series clock to deliver the best possible NTP timestamps. At line speed, NTP client packets are identified, the precise and accurate T2 and T3 timestamps are added, and the packet is returned to the requesting NTP client. Since all operations are in hardware operating at 1 GbE line speed, the NTP packet capacity is in excess of 360,000 NTP packets per second. The NTP Reflector is user-selectable with simultaneous operation across ports 2/3/4, and the optional 10 GbE ports, when the Security Protocol option is enabled. Cumulative capacity remains at 360,000 requests per second.

Advantages of NTP Reflector vs. NTP Daemon

The NTP Reflector supports the most common NTP mode 3 client requests for time. The NTP daemon running on the embedded CPU, on the other hand, is capable of more NTP features and functions. The advantage of the SyncServer S600 series is that it can simultaneously perform NTP Reflector operations on one or more user-selected ports while conducting traditional NTP daemon operations on the other ports. This provides the best of both NTP operational models, including common NTP daemon functions such as peering, clustering, selection, and MD5/SHA/AES authentication. The following table shows the primary trade-offs between using the NTP Reflector and the NTP daemon.

Note: *NTP 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. Packet limiting and alarming are discussed in detail later in this document.*

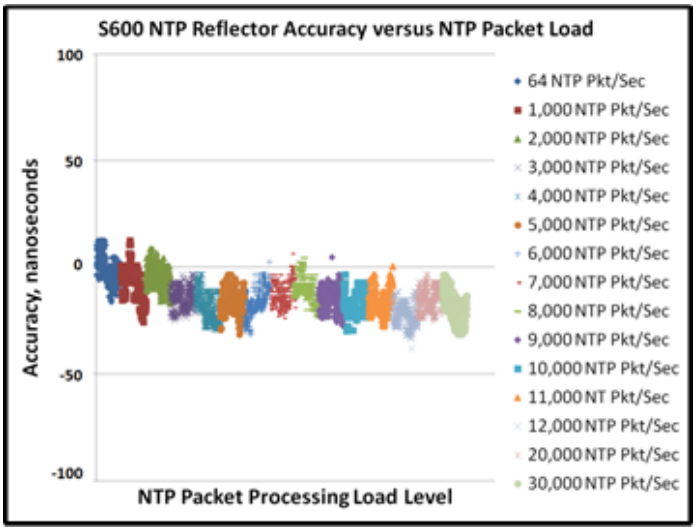
SyncServer S600 Series NTP Operations

Feature	NTP Reflector	NTP Daemon
Enhanced Security	+	–
360,000 NTP requests/second	+	–
Best Possible Timestamp Accuracy (T2 and T3)	+	–
Denial of Service Detection/ Alarming	+	–
CPU Protection	+	–
NTP Peering, Clustering, Selection	–	+
MD5/SHA and Autokey Functions	–	+

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 time stamping. This means the NTP daemon requests timestamps 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 one direction than another), varies 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.

In the chart below, 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 ns RMS to UTC independent of NTP request load. There are also no dropped packets as 100% of all NTP requests for time are responded to. This NTP timing accuracy and reliability is maintained all the way up to the full 1 GbE line speed at 360,000 NTP requests per second.



SyncServer S600 Series CPU Protection

The SyncServer S600 series 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 Microchip-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 Denial-of-Service Protection

The advantage of this multilayer protection configuration is that it protects the S600 series server from many of the effects of a DoS attack. This does not mean that a service-affecting DoS attack cannot be directed at the SyncServer 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 SyncServer 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 SyncServer 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 LAN port selected to provide NTP Reflector services is also 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 LAN port. However, if the NTP client request load exceeds the user-set threshold, an SNMP trap is sent notifying the user that the load is beyond expected levels. NTP services from the NTP Reflector are limited only by the GbE throughput of the network link.

Authentication Hardening With the Security Protocol License

Client authentication hardening—whether client, server, or user access—is another level in security hardening. Included with the Security Protocol License is the NTP Autokey functionality. For user authentication/permission, TACACS+, RADIUS, LDAP, and X.509 certificates are also supported.

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 timestamp 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.

Security Protocol License Option

The NTP Reflector and packet limiting/monitoring is part of the SyncServer S600 series Security Protocol License. All SyncServer S600/S650 models are equipped with all of the necessary hardware to perform the functions mentioned in this application note. The NTP Reflector features are enabled through the separately purchased Security Protocol License option delivered as a license code that can be entered in the web interface either at the time of initial purchase or anytime thereafter.