The Global Leader in Resilient **PNT**

Technical Note: NTP Time Server

NTP Server Capacity Testing

Introduction

Large-scale NTP deployments require consideration for the network's time synchronization architecture. Network time deployments are usually driven by considerations for reliability, scalability, manageability, and security. The capability of modern NTP servers, such as Orolia SecureSync® and NetClock® time servers, is such that capacity does not impact the design of the synchronization architecture. But it is good to know the limits of capacity of the NTP server. This Technical Note describes test procedures to determine the NTP request threshold of Orolia SecureSync and NetClock and to determine and describe quantitatively the maximum number of NTP requests that can be serviced by these devices in unit time.

Overview

To test the number of NTP requests that can be handled by the time server, we have developed a tool (NtpStress.exe) that can send large number of NTP requests to the unit and measure the maximum number of requests serviced. Tests were performed for two different scenarios and were performed without any form of packet authentication.

Equipment

The hosts are a computer with a 1 Gigabit network interface card (NIC) running Orolia's test software tool NtpStress.exe. A 1 Gigabit Switch was used to connect the host(s) to a SecureSync Time and Frequency Synchronization System via Standard Ethernet cables.

Test Scenario 1: Single Host

This test was performed to measure the number of NTP requests that can be serviced by the unit when the requests come from a single host. In this setup the host and the unit were connected to a simple network via a switch to minimize network delays and losses and thus the NTP request threshold of the SecureSync can be accurately determined.

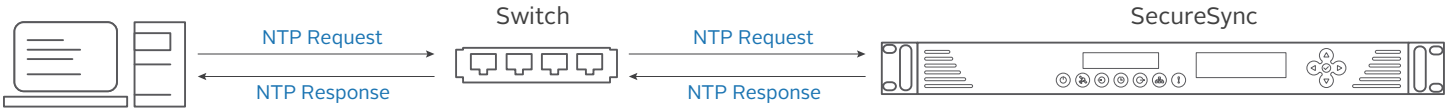

Figure 1: Testing NTP Request Threshold with a Single Host

Test Scenario 2: Multiple Hosts

The second test is designed to be carried out with multiple hosts sending NTP requests to the unit over a network. It consists of three hosts connected to a simple network via a switch, which is also connected to the unit, to increase the amount of packets sent to replicate a standard network configuration and estimate the NTP requests per second threshold. The time delay between starting the tool on multiple hosts should be kept to a minimum. To get more accurate results with multiple hosts, the time duration of the test should be kept large enough to negate the effects of any time delays during startup, such as 2-5 minutes.

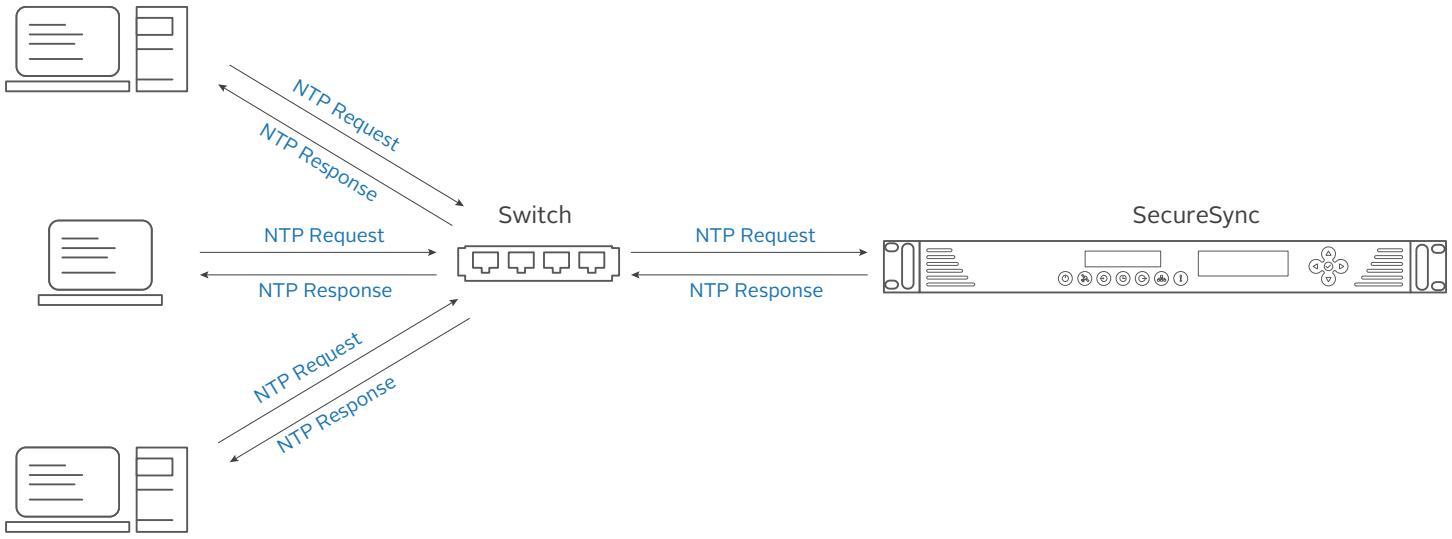

Figure 2: Testing NTP Request Threshold with Multiple Hosts

Test Software

The NtpStress tool initiates a test with a simple command, example: ntpstress 10.10.10.1 1000 60. The first parameter is the IP address of the NTP server under test. The second is the desired number of NTP requests per second. The third is the total test length in seconds. A fourth parameter can be specified at the end to name the report file other than the default of ntpdata.txt. A detailed status report is written to this file.

After the test is completed, the tool will output the results as shown:

```
Average NTP Req/Sec:    992
Total Requests:         9917
Failed Requests:        0
Bad Stratum Level:      0
```

The output above shows Average NTP Req/Sec which is the main result required by this test. This means that the SecureSync was able to service 992 NTP Requests/second.

Results

The results obtained in a test of a single host (laptop with Windows 7 and 1 Gigabit network interface) is as follows.

NTP requests specified (per second)	Time Duration (Seconds)	Average NTP requests serviced (per second)
1.000	60	1.000
3.000	60	2.371
4.000	60	3.548
5.000	60	4.321
6.000	60	4.377
10.000	60	4.484

Table 1: Test Results with a Single Host

It can be seen from the above results that the number of NTP requests per second serviced by the unit saturates close to 4,500 Req/sec. A test of multiple hosts reveals that this limit is due to ability of the host to generate requests.

		Average NTP requests serviced (per second)			
NTP requests specified (per host, per second)	Time Duration (Seconds)	Laptop (10/100M) Windows XP	Laptop (1 Gigabit) Windows 7	PC (10/100M) Windows XP	Total
10.000	100	2.452	3.502	3.929	9.883
50.000	100	2.415	2.449	4.131	8.995
50.000	100	2.428	2.459	4.137	9.024
50.000	100	2.374	3.457	3.945	9.776
90.000	100	2.448	3.518	3.943	9.909

Table 2: Test Results with Multiple Hosts

With three hosts sending NTP requests to the SecureSync on a small network, the unit was able to service up to a maximum of 9,909 NTP requests per second.

NTP Throughput as a Function of Internal Configuration

Orolia continually evolves its time server platform to add features, improve reliability and patch security vulnerabilities. These updates can affect components such as the network controller and its associated driver. These components can impact NTP throughput. Testing performed on an updated configuration in 2016 showed a reduction in the number of NTP requests serviced to about 7,500. Securesync 2400 Base supports up to 7500 NTP requests per second. Option Card, 1204-49 or 1204-4A, have their own NTP processing capability (similar to the base unit), adds 7500 requests per second.

For example :

Securesync 2400 Base unit + one 1204-49 OC provides 15 000 requests per second.

Securesync 2400 Base unit + two 1204-49 OC provides 22 500 requests per second.

Conclusion

The Orolia NTP service implemented on SecureSync and NetClock 9400 was tested to determine its NTP requests per second threshold value without authentication. Specific software components can affect throughput. An earlier configuration was capable of up to 9,909 NTP requests per second. An updated configuration was able to serve approximately 7,500 NTP requests per second. Adding option card will increase the throughput up to 22500 requests per second. Since these values are sufficiently large for most applications, Orolia does not routinely evaluate NTP throughput in its regression testing for product updates and new software releases. However, Orolia can routinely perform this testing if it is helpful for the planning of a specific NTP deployment.

www.orolia.com
sales@orolia.com

2 June 2022 - TN19-101 (C)