The Global Leader in Resilient **PNT**

Technical Note: Network Master Clocks and Time Servers

Routing of Data Across Multiple Networks

Orolia's SecureSync® and NetClock® timing appliances have a built-in 10/100 base-T network port for set-up, management and operation of network time protocol (NTP). These systems can be expanded by a 3x 10/100/1000 multi-port module to leverage network functionality across multiple LAN segments. Where security is the driver for network segmentation, it is important to understand the degree of isolation between segments managed by a single system. This note provides a general description of the software routing scheme of a single Orolia unit with multiple network ports and offers alternative timing hardware deployments if software isolation is insufficient.

Introduction:

First it is helpful to understand that the function of a Orolia device inherently limits security risk by its function as a timing device. It does not have the ability to store, nor pass, any data other than its configuration, status, and what is supported by network time protocol (NTP) and any other enabled network service (all network services can be individually enabled and disabled). Incoming packets will be supported given proper authentication of user credentials or other security infrastructure supported by the unit. However, fundamental to the design is that all functions handled by the built-in 10/100 port and each port on the multi-port module run on a single processor and they share the same network stack. A routing scheme is used to control port isolation.

Set-up and operation of multiple network ports:

When the multiple network port module is installed in a SecureSync or NetClock unit, each network interface is independently enabled and disabled, and configurable with an IP address and a default gateway (if so desired). Each port has a unique routing table and is governed by a rule that all incoming requests are responded by that port according to the routing table. This approach provides software-based port isolation.

Let's use a basic example to show how routing works and then describe how internally generated network messages are directed. First, consider a Orolia device with a single network port. That device manages messages typical of any network host. It directly addresses any other host on its subnet and sends messages to hosts on other subnets via a gateway. Additionally static routes can be configured. The combination of the subnet, gateway and static routes can be thought of as a routing table for the port.

If a unit is configured with the multi-port network module then each port has a unique routing table including its subnet and gateway configuration plus any static routes that have been configured for that port. So with 4 network ports, there are 4 unique routing tables. The only time these routes are combined is for routing system-generated messages that are not in response to an external request such as SNMP traps. A fifth routing table is used for those messages. This table known as 'main' is the sum of all the routes configured for each port with the exception of the gateway. Only one of the 4 potentially available gateway addresses can be defined as the 'main' gateway and used for routing when no other route exists.

As an example of an IPv4 deployment and given the following network settings:

Designator	eth0	eth1	eth2	eth3
Port IP address	10.10.2.1	10.2.3.1	192.168.1.24	10.0.4.5
Subnet prefix	16	16	16	16
Gateway	10.10.1.1	10.2.1.1	192.168.1.1	10.0.1.1

The routing tables are defined as (in the absence of any static routes):

t0	t1	t2	t3	main
10.10.x.x/16 via eth0	10.2.x.x/16 via eth1	192.168.x.x/16 via eth2	10.0.x.x/16 via eth3	10.10.x.x/16 via eth0 10.2.x.x/16 via eth1 192.168.x.x/16 via eth2 10.0.x.x/16 via eth3
Default 10.10.1.1 via eth0	Default 10.2.1.1 via eth1	Default 192.168.1.1 via eth2	Default 10.0.1.1 via eth3	Default, one of: t0, t1, t2, t3

Any inbound request directed to 10.10.2.1 is responded to according to t0, and so on. Any system generated network message is routed according to 'main'. The route (and port) is selected based on the destination address. If no route matches the destination address, then it is sent to the default gateway that is user-configurable from the 4 available (and from the port defined by that gateway).

Alternatives for greater isolation via hardware:

There are 3 deployment scenarios to achieve hardware isolation between ports with a Orolia timing system. The first scenario uses an option module design with a unique processor and network stack to perform a specific network function. This design is currently available on two different precision time protocol (PTP) modules. One has PTP master/slave capability via a 10/100 RJ45 interface. The other is via 1 GbE on an SFP module. This architecture could be deployed for other network functions.

A second and third scenario involves multiple units, each with a single network port, while dedicating the master clock functions to one. For many years, Orolia has used precision time code via unidirectional RS485 communication to synchronize a single master to multiple slave units capable of NTP stratum-1 operation. This approach is relatively low-cost and can offer physical isolation as well as processor-network hardware isolation, but requires 1RU for each port and does not offer complete electrically isolation. For the most sensitive deployments that require physical and electrical isolation, crossing classified and unclassified red-black networks can be achieved through optical signals via fiber in a similar master-slave combination. SecureSync units can be configured with built-in optical interfaces for a master-slave configuration. IRIG timecode, 1-way communication, is recommended.

13 February, 2019 - TN25-101 (B)