Advanced Network Tap application for Flight Test Instrumentation Systems

Ø. Holmeide[1], M. Schmitz[2]
1 OnTime Networks AS, Oslo, Norway
oeyvind@ontimenet.com
2 OnTime Networks AS, Dallas, USA
markus@ontimenet.com

Abstract:

Digital data distribution systems are widely used in Aerospace and Defense products to allow devices to communicate with one another. In many cases it is desirable to monitor the data traffic flowing between two points in a copper or fiber based Operational or Onboard Network System (ONS) for Flight Test Instrumentation (FTI) purposes because these ONS systems may carry important data which can be used without duplicating/installing a specific FTI data acquisition system to receive this data. The two types of network taps that can be used are Inline Network Taps and network end-point taps. This paper examines the usage of Inline Network Taps for FTI applications and how they can support network access strategies and objectives. An Inline Network Tap is a hardware device which allows access to data flowing across a network. These devices are typically active/powered and have a number of ports: a first tap port, a second tap port, and one or more mirror ports. An in-line network tap inserted between the first and second tap port passes all data traffic through unimpeded but also copies that same data to one or more mirror ports. Some Inline Network Tap devices may also pass packets when the tap is not powered or a malfunction is detected on the device via an integrated by-pass function. If the Inline Network Tap device goes offline the unit automatically bypasses the tap connection and data traffic is directed through the bypass directly to network devices. This capability is crucial for inline usage on mission critical network segments that cannot afford the risk of losing the network connection. An in-line network tap can either be based on copper or fiber technology and as a "filterable" network tap can also provide advanced packet filtering capabilities. These filterable network taps can selectively pass data, e.g., based on VLAN ID or other parameters, to a mirror port for deep analysis, monitoring and recording. Another advanced tap function that is presented in this paper is the support for inserting time stamps at the tap level in monitored packets which provides a reference time when the data content of a given packet was generated at a data source[1]. This capability is a significant feature for FTI applications as most ONS systems do not provide time stamped data.

Keywords: Network tap, time stamping, IEEE 1588, FTI

[1] Patent pending

Introduction

This paper describes the main principles of an Advanced Network Tap, where data packets are passed through the device regardless whether the device is powered or the device is operating as an active network tap, where data packets are mirrored to one more port mirror ports. The paper also describes how advanced packets filtering techniques can be used in order to limit the amount of data mirrored to the mirror ports as well as time stamping data packets and inserting the precise time stamps into the mirror data packets.

Advanced Network Tap - Principle of Operation

The Advanced Network Tap can operate in two modes: BYPASS and TAP mode. Packets in both modes will be forwarded between the two tap ports. The Advanced Network Tap will be in BYPASS mode when:

- The device is without power,
- Is booting, or
- A malfunction is detected on the Advanced Network Tap

The Advanced Network Tap will enter TAP mode after boot is completed and if the Built-In-Test (BIT) is successful, links are found on both tap ports, speed and duplex connectivity are the same for the two tap ports and the Network Tap prior to the last power loss was in TAP mode.

The user can select to use one or two mirror ports. Packets received on tap port 1 (J1) are mirrored to mirror port J3 and packets received on tap port 2 (J2) are mirrored to mirror port J4 in case two mirror ports are used.

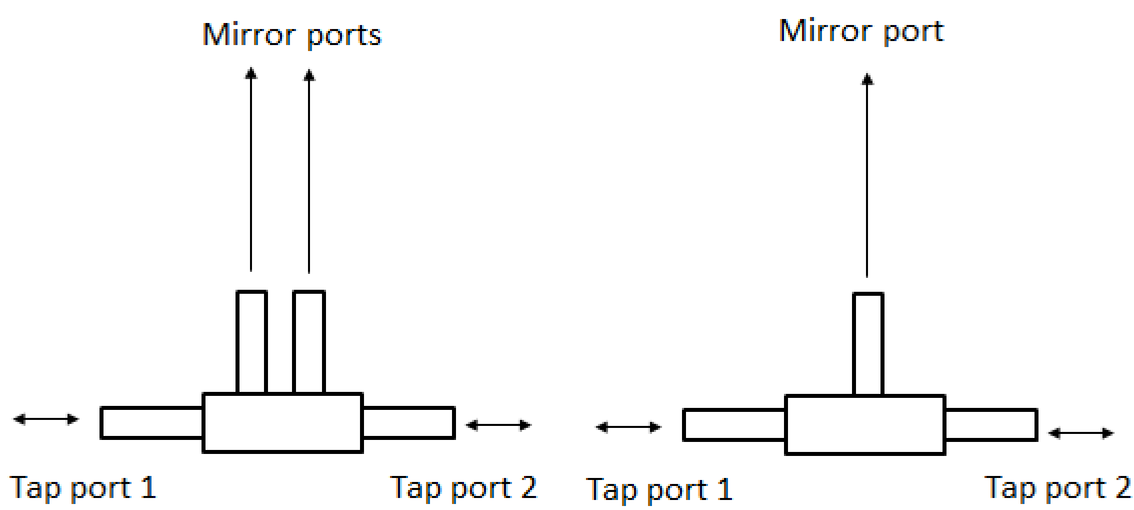

Figure 1, Network taps with one or two monitoring port

The user may also issue a management reset command to the Advanced Network Tap if the device has entered BYPASS mode. The Advanced Network Tap will then enter TAP mode if BIT is successful, links are found on both tap ports and speed and duplex connectivity are the same for the two tap ports. The reason for this function is to minimize the number mode changes on the Advanced Network Tap since a mode change represent link re-training on the tap ports with some packet loss as a result.

Switch Port Mirroring vs Network Tap

It has been a questionable practice for FTI applications to utilize *Switch Port Mirroring* as a way to access data flow across a network. Many Ethernet switches (but not all) provide *Switch Port Mirroring*, but the user should know that the switch packet scheduler will grant the *Switch Port Mirroring* function with the lowest possible priority. The *Switch Port Mirroring* function is the first function that will be disabled in case of e.g. network congestion, with packet loss on the monitoring port as a result. In addition *Switch Port Mirroring* might require switch resources that can load the unit and lead to reduced switching performance. Further, a switch with port mirroring is a point of failure, in case of power loss or a switch malfunction.

Latency Aspects of Inline Taps

The Inline Tap will increase the network latency, but the network tap latency in case the Inline Tap is running in TAP mode, will not depend on the network load on the Inline Tap. The whole egress bandwidth of tap port 1 is allocated to the ingress data received on the tap port 2 and vice versa. This means that there is not latency jitter introduced due to packet queueing as would have been the case for a standard switch where packets originating from several ingress ports may be forwarded and queued to the same egress port. The Inline Tap latency depends on the port speed, packet length and a general static latency of a few microseconds. The network tap latency in case the Inline Tap is running in BYPASS mode, is close to zero.

No Traffic flow back into the operational network

The mirror ports of the Inline Tap can receive data, but this data can only be sent to the CPU of the Inline Tap. As the consequence, a mirror port can also be used for management of the Inline Tap, while data from the FTI system cannot flow back into the ONS system. The mirror ports do not have the capability to receive packets and send them into the ONS network.

Packet filtering

Packet filtering of mirrored data packets may be relevant in order to limit the amount of data sent to e.g. a recorder.

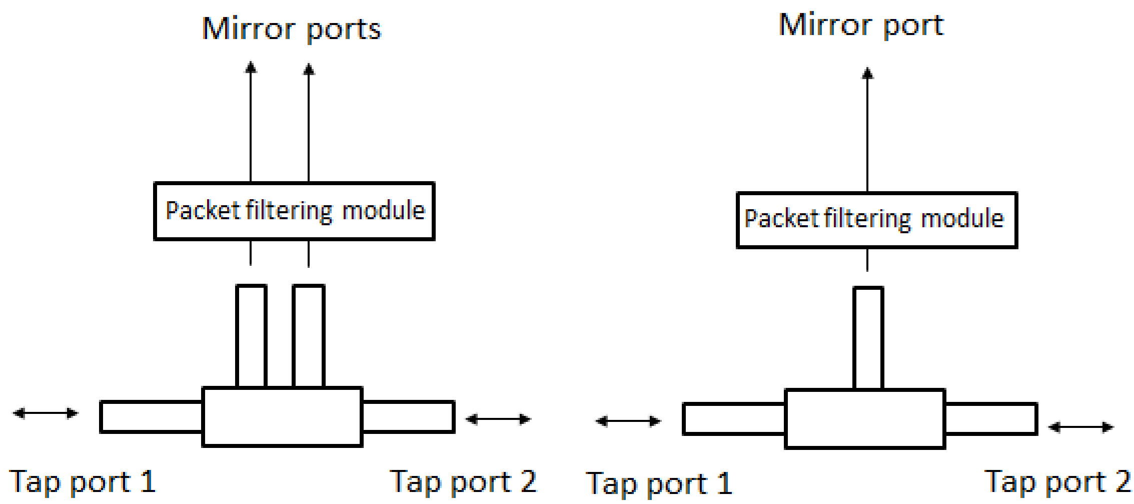

Figure 2, Network taps with packet filtering

A "filterable" network tap, which is commonly-used in a 10 Gigabit environment, provides advanced filtering. It can selectively pass data, e.g., based on application, VLAN ID, or other parameters, to a 1-Gigabit port for deep analysis and monitoring. Once a network tap is in place, the network can be monitored without interfering with the network itself.

It is also possible to insert another filtering device in-between the Advanced Network Tap and the recorder(s), where packet filtering is based on IP protocol header (layer 3), UDP header (layer 4) or even the content the packet payload, i.e. an End-Point Tap. See [1] for more details. Such a filtering device can also split the data stream into several streams based on e.g. source IP addresses as a filtering criteria in order to record different data on several recorders.

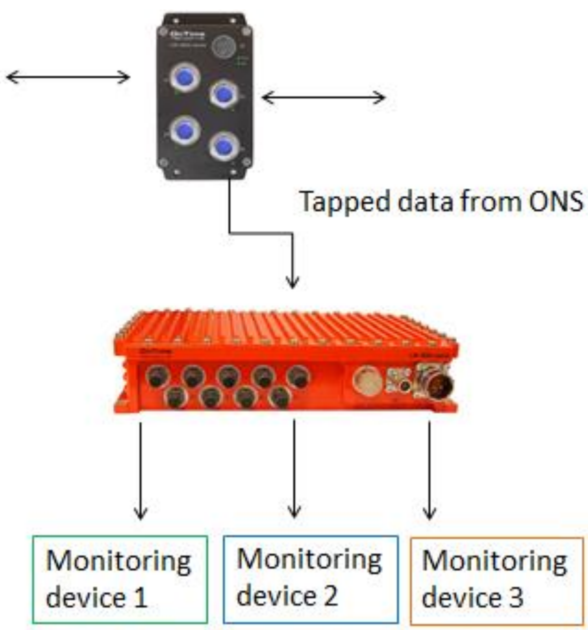

Figure 3, Network tap + End-point Tap

Advance Network Tap and Time Stamping of Mirrored Data

In the context of a network tap that implements the IEEE1588 standard, the clock used for time stamp generation can be based on a PTP Slave Clock implementation or an NTP/SNTP client implementation.

Time Stamping of Mirrored Data becomes critical if the tapped data is not directly sent to a recorder for recording or the recorder is not capable of performing precise time stamping of the data packets. In the scenario that a FTI system has to tap multiple Tap lines and this data is send via the FTI network to the recorder, it is necessary to time stamp the tapped data as close to the source as possible, in order to allow precise analysis of the data. In cases where the tapped data is already time stamped by the tapped ONS system no further time stamping will be required, but in cases where the tapped data is not time stamped, OnTime Networks can provide a Network Tap solution with the capability of time stamping the data close to the wire. The time stamp for the tapped data is inserted by a time stamp module. The time stamp module generates a time stamp and inserts the time stamp in the packet, either in the packet header or in the packet payload. The time stamp represents the “time” when the contents of the data packet (in the data packet) is considered to be generated at a sending node from which the tapped data originates. Preferably, and before being inserted into the packet, the time stamp generated for a particular packet is adjusted for the propagation delay between the sending node and the network tap element. In addition, the time stamp may be adjusted for a time differences between when the packet was sent and when the data packet content was generated at the sending node. In either case, after the time stamp module inserts the time stamp in the packet, the module preferably recalculates or sets to zero a UDP checksum (if the received packet is a UDP packet and the time stamp is inserted in the UDP payload), and recalculates and inserts a new MAC checksum in the packet.

Conclusion

This paper addressed the benefits of using dedicated Advanced Network Taps for Flight Test Instrumentation System applications. We identify that when monitoring network links in FTI systems it is recommended to use advanced network tap devices to mirror and analyze high-speed connections, as these devices provide significant benefits over the use of port mirroring. We looked at the different operation principles of network taps, touched the use of packet filtering techniques and evaluated latency aspects of Inline Taps. The findings clearly show that these aspects are in line with FTI network requirements and provide significant advantages. Further, the introduction of by-pass relays into the design of rugged network taps allows the use of these devices for tapping of more critical links, which to less extent can be interrupted by power loss or malfunctions. We have also evaluated the risk of traffic flow back into ONS and learned that specific design principles of Inline Taps will eliminated this risk. With the increased usage of Ethernet networks within the Aerospace and Defense industry in airborne, ground or naval applications, the need to tap, monitor and analyze network traffic has increased and will continue to rise going forward. We also foresee that Time Stamping of Mirrored Data by Inline Tap devices will become an important functionality, which can help with analyzing network data if multiple taps are used or the tapped data flows through a network. Considering all this, we believe that going forward advanced network taps will be a standard tool in every FTI engineer's tool box.

References

[1] Holmeide, Gauvin: "c for FTI - part I"