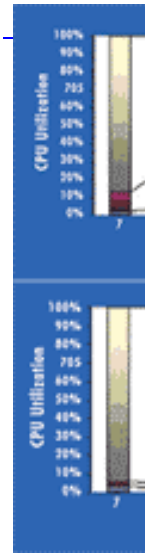
Tuning Ethernet for Military Networks

In addition to predictable performance, reliability is a key requirement for any military network.

Steve Rood Goldman, Data Device Corporation

The DoD's Net-centric Warfare initiative ensures that IP networks and Ethernet are here to stay. Ethernet is being deployed or implemented in a number of military



[1]

systems including transport, reconnaissance, bomber, UAV and rotary wing aircraft; army ground vehicles; as well as multiple navy vessels. But for many military applications, Ethernet is not a drop in solution. As examples, sensor interfacing and control applications generate bursty, latency sensitive network traffic that may be incompatible with some Ethernet implementations.

Ethernet physical and link layer protocols are managed by dedicated computer system hardware, while upper level protocols, including TCP/IP and UDP/IP, are handled by processor software. For low speed connections there is processor bandwidth to spare. As military applications transition to Gigabit speed, embedded processors may have insufficient resources to handle the additional processing overhead, resulting in throughput limitations and data jitter. Protocol offloading and co-processing techniques offer an alternative to boosting overall processor performance to meet network performance requirements. Offloading addresses performance limitations by providing hardware assist to the host processor in handling network protocol processing, while co-processing can be used to handle all or part of the network application.

Ethernet Protocol Processing

To demonstrate the severity of the loading imposed by Ethernet protocol processing, measurements were made using two military single board computers (SBC) based on a 1 GHz 7455 PowerPC processor. Both SBCs were running the VxWorks 5.5 real-time operating system. The integrated Gigabit Ethernet ports on the SBCs were connected through a managed switch for monitoring purposes. One SBC was used as the data transmitter and the other as the receiver. CPU loading was monitored as throughput was varied by adjusting message and data buffer sizes. In order to roughly simulate the behavior of an embedded system, a mission function was used to occupy as much of the CPU as possible by calculating the roots of polynomials.

As shown in Figure 1a, the impact of the operating system kernel task remains nearly flat as throughput is increased. The NetTask, which includes the operation of the TCP/IP protocol stack, increases with throughput such that close to the full capacity of the processor is used to receive data packets at greater than 50MB/s.

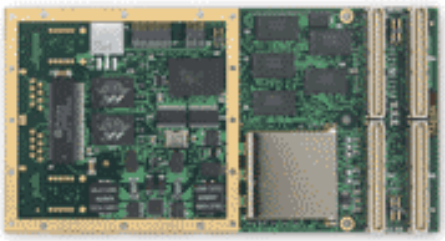
Figure 1b shows the effect of using a TCP/IP Offload Engine (TOE) device in place of the SBC's integrated Ethernet port. In this case, less than 10% of the processor is used by the NetTask, leaving most of the capacity for the mission function.

Figure 2 shows an example TOE device, the DDC ET-71000 Gigabit Ethernet Network Access Controller. This mezzanine card, designed for rugged military applications, uses a processor-based TOE implementation to provide full, transparent offload of the protocol stack. Compared to commercial Ethernet controllers, the processor supports extended temperature operation and provides the flexibility needed to incorporate enhanced QoS and redundancy protocols.

Improved Reliability

Another performance-related limitation of IP-based Ethernet networks is that they provide best effort service. This means that there are no throughput or delay guarantees. While IP provides a means of tagging traffic priority, additional protocols are needed to classify and manage the traffic.

Differentiated Services, used in commercial IP networks, uses a small number of priority classes to statistically allocate network bandwidth. DiffServ is not a good option for military applications that



require guaranteed delay bounds. Integrated Services protocol manages individual flows through the network and can provide service guarantees. But this fine-grained management approach requires that all routers on the network implement IntServ protocol and store state information for each flow. Storage overhead increases as the network scales, making IntServ

expensive for large commercial networks, but practical for smaller, closed military networks.

The commercial aircraft industry has begun to implement networks based on ARINC 664 standard, a profiled version of 10/100 Mbps Ethernet, which provides bandwidth management and redundancy features. By setting a maximum frame size and inserting gaps between frames, ARINC 664 is able to control the network bandwidth allocated to individual avionics subsystems. In this way, an errant subsystem cannot impact another subsystem.

In addition to predictable performance, reliability is a key requirement for any military network. Redundancy mechanisms can be used to ensure high availability of Ethernet IP networks. Transaction Control Protocol (TCP) provides temporal redundancy by resending unacknowledged packets, but TCP retries can lead to network congestion and unpredictable delays. Protocols such as Rapid Spanning Tree Protocol (RSTP) and Link Aggregation Control Protocol (LACP) are used to provide redundancy in commercial networks, but take on the order of seconds to respond to link failures. Military systems require more rapid recovery techniques to prevent data loss.

ARINC 664 provides dual-redundancy by simultaneously transmitting traffic over two independent paths. Errors are detected at the receiver, which then identifies and discards duplicate data packets. Error detection and recovery is entirely transparent to the network application. Because there is no failover time or data loss with this redundancy approach, it should be well-suited for military networks.

Conclusion

The growing interest in Ethernet for Military applications has been driven by the networking technology's commercial success, but military system designers cannot always achieve satisfactory results by the reuse of commercial Gigabit Ethernet products. Stringent performance bounds set military applications apart. Nevertheless, technology originally driven by commercial applications including host offload and quality of service protocols are a good starting point for a solution and should be adapted to military use.

About the Author

Steve Rood Goldman is product manager for Data Device Corporation, 105 Wilbur Place, Bohemia, NY; (631) 567-5600; www.ddc-web.com.

Source URL (retrieved on *07/28/2014 - 7:22am*):
http://www.wirelessdesignmag.com/product-releases/2007/03/tuning-ethernet-military-networks?qt-digital_editions=0

Links:

[1] http://www.wirelessdesignmag.com/sites/wirelessdesignmag.com/files/legacyimages/0703/datadevice1_lrg.gif