GUARANTEED QUALITY OF SERVICE INTERNETWORKING FOR INTEGRATING DISTRIBUTED INTERACTIVE SIMULATIONS WITH THE TELEMETRY RANGE

Dr. Gary Rucinski

BBN Systems and Technologies

ABSTRACT

In recent years the extension of interactive simulation technology to involve simulators and live vehicles from geographically dispersed sites has produced a demand for high-bandwidth communication networks that can provide guaranteed quality of service (e.g., insured availability of bandwidth and upper bounds on end-to-end delay). This paper reviews the requirements distributed interactive simulation places on the communications infrastructure and describes the Defense Simulation Internet (DSI), a network developed by the Advanced Research Projects Agency to support distributed interactive simulations. Key features of the DSI are: more than 120 participating sites spanning Europe, the United States and Asia; use of a resource reservation mechanism to provide guaranteed quality of service; and support for communication between classified sites. Furthermore, the paper describes the internetworking protocols used in the DSI to provide guaranteed quality of service and to support transmission of classified communications. Other topics discussed in the paper are research efforts that anticipate increased load on the DSI and the relevance of the technology to the integration of the telemetry range and distributed interactive simulations.

KEY WORDS

Telemetry Range Internetting, Distributed Interactive Simulation, Virtual Range

INTRODUCTION

The telemetry range of the future will have many new capabilities to make range operations more cost effective and to expand the scope of exercises that can be supported. As one example, cost savings will be gained by range interconnection via packet-switched networking technology. These cost savings will occur because range internetting will permit sharing of fixed resources, such as data acquisition and

monitoring equipment. Range internetting will also support instantaneous distribution of real-time data, facilitating active participation of government or contractor personnel from other sites in the planning, execution and analysis of tests. Integration of tests at different ranges and integration of data from live vehicles with interactive simulations are other areas under active investigation. Introduction of advanced internetworking technology will improve capabilities in all of these areas.

In order to support these new capabilities, internetworking technology must be able to meet certain basic requirements. These include:

Wide Area Internetworking: This technology enables packet-switched internetworking over long distances, typically across continents or around the globe.

Secure Communications: Range internetting will not be useful unless it is possible to utilize encryption technology to enable exchange of protected, classified information over unclassified Wide Area Network (WAN) communication links.

Guaranteed Quality of Service (QoS): Many of the applications that will be of interest to telemetry range operators and users will require reliable delivery of real-time data over the packet switched network. A mechanism must be provided for telemetry range applications to reserve network resources in advance in order to insure that packets are always delivered to their destinations and that relevant real-time constraints are satisfied.

STATE-OF-THE-ART INTERNETWORKING TECHNOLOGY

The requirements for supporting the telemetry range of the future can be met with internetting technology available, and in use, today.

Wide area internetworking technology has been available for several years. Today, conventional WANs are capable of operating at speeds of 45MBits/second. The introduction of Asynchronous Transfer Mode (ATM) technology will push this to 600MBits/second and beyond. These rates are more than adequate to support several range internetting applications.

The existence of many forms of encryption devices operating at internetworking speeds, or several devices operating in parallel, ensures that encrypted classified data can be transmitted at reasonably high rates over unclassified transmission lines. Unencumbered exchange of classified data removes a major impediment to cooperation and resource sharing among ranges and contractors.

Resource reservation internetworking protocols are now available for supporting QoS guarantees in a packet switching environment. Resource reservation protocols provide applications with mechanisms to reserve network resources required to handle their data flows all along the path from source to destination. The simplest reservation that could be made might be for throughput, such as a guarantee that a particular packet rate or bit rate will be supported. QoS guarantees could also apply to constraints on end to-end delay or variation in interpacket arrival times. Given a prior notification of a need for transmission bandwidth contained in a reservation request, intermediate network nodes (i.e., gateways) can anticipate future load and, by avoiding oversubscription, support the resource reservation.

The support for resource reservation can be contrasted with the more familiar best effort service provided by the Internetwork Protocol (IP) and other conventional protocols. There are no service guarantees when using IP. The network is said to make its "best effort" to deliver all packets. Because IP does not provide service guarantees, IP packets may not reach their destinations if congestion develops within the network. In the presence of congestion, transmission and receive queues overflow and packets get dropped. Any application that requires reliable data transmission must be written to achieve that goal itself, typically by marking packets with sequence numbers, tracking sequence numbers of packets as they arrive at the destination and requesting retransmission of packets when gaps are detected.

While the technological building blocks exist today to build a range internetting infrastructure, not all of the necessary system components are capable of operating at required levels of performance. For example, systems which implement resource reservation protocols do not yet operate at WAN speeds quoted above. Also, because of processing overhead associated with encryption, security equipment represents a significant bottleneck. Nonetheless, the performance of internetworking components is constantly improving and systems that meet operational requirements have been developed as the next section describes.

THE DEFENSE SIMULATION INTERNET: A WORKING EXAMPLE

In recent years the military has increased its reliance on Distributed Interactive Simulation (DIS) [1,2] as a means of providing troops with adequate opportunities for training and as a tool for weapon system development and research (Figure 1). Initially simulators used in DIS were co-located and connected by Ethernet. It was soon realized, however, that significant savings could be achieved, simultaneously with expanding the scope of training exercises and new weapons research, by installing simulators at many sites around the world and connecting them using wide-area, packet-switched networks (Figure 2). In order to support this expansion to

wide-area communications, however, the packet-switched network had to meet the requirements of real-time data communication between geographically-dispersed sites.

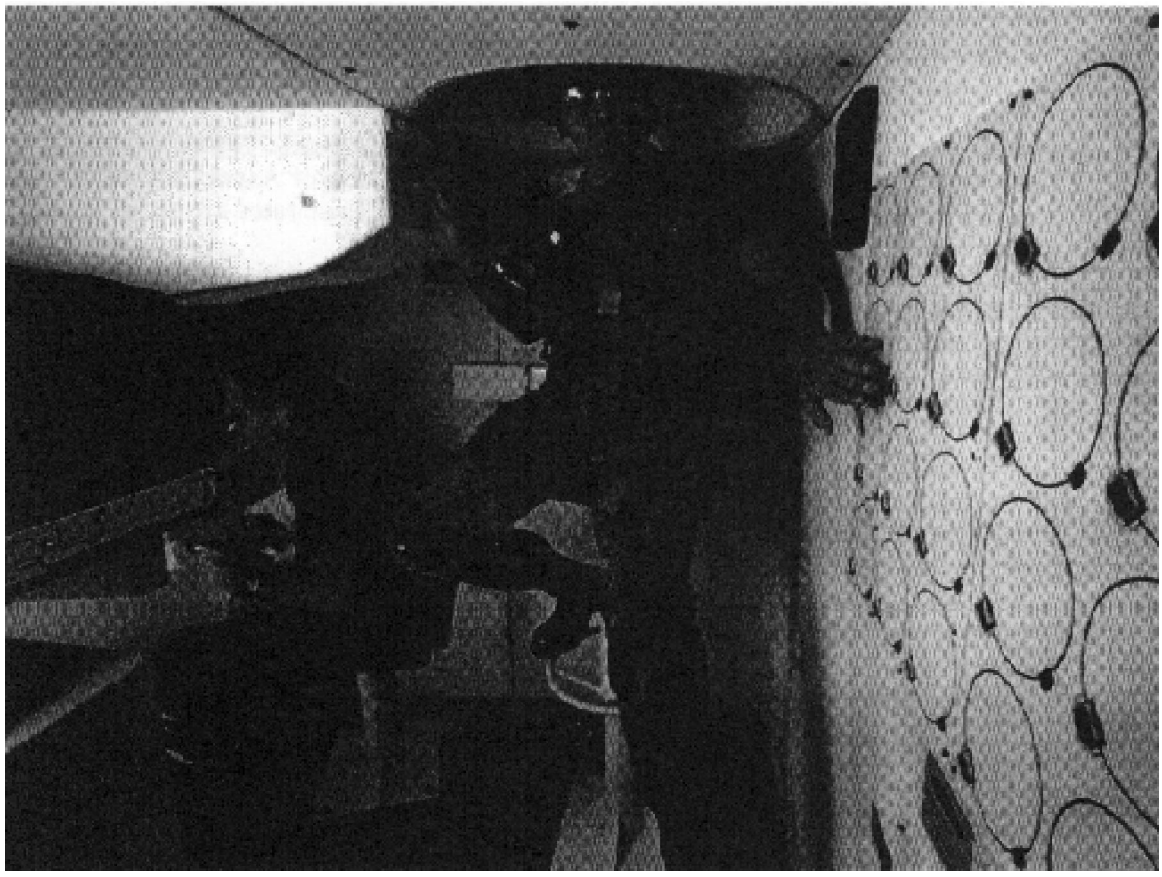

Figure 1. Photograph of a manned, interactive simulator used in DIS

The Advanced Research Projects Agency (ARPA) has developed a network that meets the communication requirements of DIS. (See Figure 3.) This network, called the Defense Simulation Internet, or DSI, has been in operation for several years. It currently spans three continents and, in addition to supporting DIS, is used for supporting Video Teleconferencing (VTC) and phone and fax communications.

The key operational requirement for the DSI is support for guaranteed QoS for data transmission over a packet-switched network. In simpler terms, distributed simulations or video teleconferences had to be guaranteed that all data would be delivered to participating sites.

The DSI achieves the goal of providing guaranteed QoS through the use of a two-tiered internetworking infrastructure. In the first tier, video teleconferencing equipment or local area simulation networks are connected to ports on BBN's T/20 Internet Packet Router (T/20 IPR). The T/20 supports the Stream Protocol Version 2

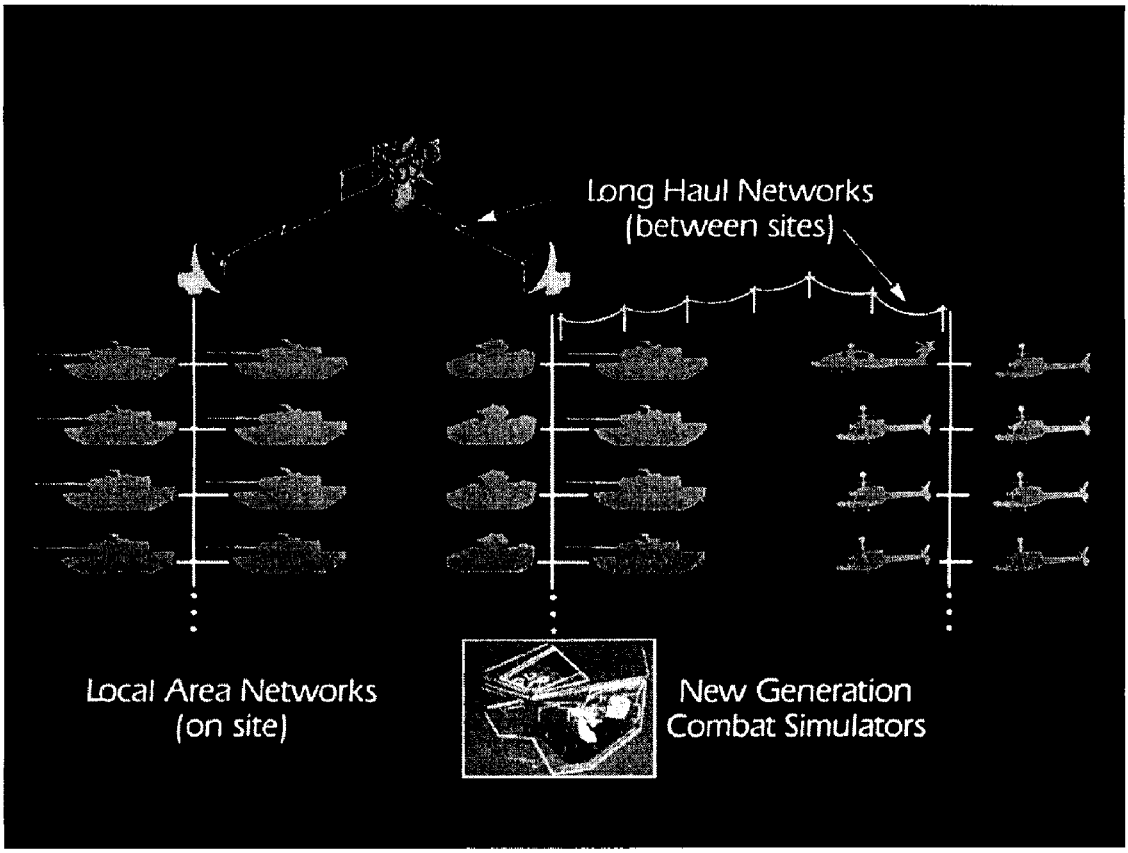

Figure 2. Schematic representation of the Distributed Interactive Simulation concept in which interactive simulators at several different sites are interconnected via a wide-area network.

[3] or ST-II (Figure 4), a resource reservation protocol developed by the Internetworking Engineering Task Force (IETF). ST-II supports the establishment of one-to-one (unicast) and one-to-many (multicast) virtual connections (or streams) between an origin and one or several targets. The protocol contains the elements required for applications to initiate reservation requests, specify the characteristics of the reservation and receive notification of success or failure by the network in establishing the connection. The T/20 IPR routes both ST-II and IP traffic through the DSI.

In the second tier, the T/20's connect to a terrestrial wide-band packet-switched network. The wide-band network is comprised of BBN Wide-band Packet Switches (WPS). The WPS's form a backbone that interconnects all T/20's on the DSI. They implement the lower layer, proprietary Host Access Protocol (HAP) which also supports QoS guarantees. Total throughput supported by the WPS backbone is 2xT1 or 3MBits/second.

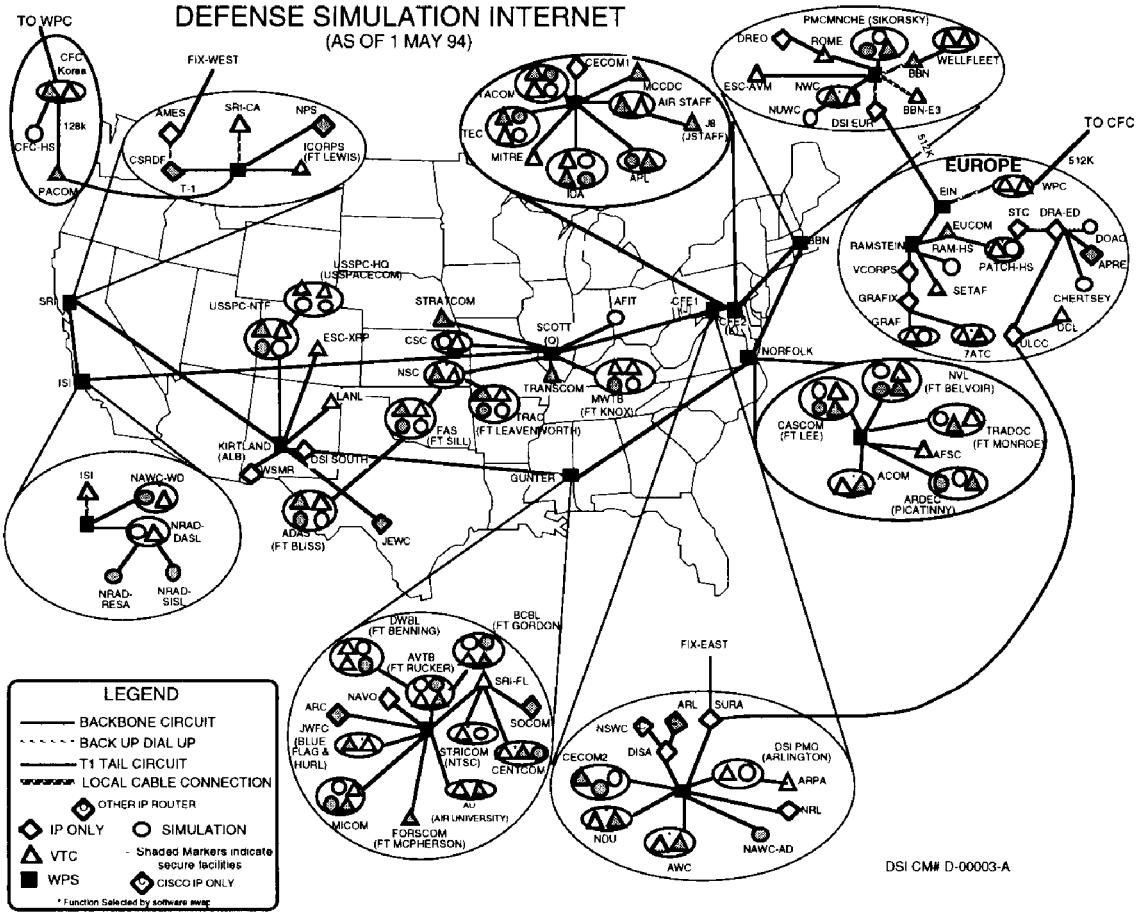

Figure 3. Map of the Defense Simulation Internet.

While the DSI uses proprietary protocols and hardware to implement the network's backbone, this function can also be supplied using non-proprietary solutions. Work in this area involving emerging Frame Relay and Asynchronous Transfer Mode protocols is already taking place. In addition, some applications will not require a backbone-based architecture, but will instead be capable of being implemented as an interconnected series or mesh of T/20's.

Application software running on the T/20 IPR establishes the ST-II streams required to support VTC's or simulations. The T/20's in turn use the HAP protocol to reserve backbone resources for the streams. The remainder of this discussion will focus on the ST-II protocol as this is the primary interface to the user and applications. Network layering in general will make the details of the backbone or other interconnection scheme transparent to higher level applications.

Once an ST-II stream is established the traffic submitted to the stream is guaranteed to be delivered as long as the application does not attempt to transmit data that is different in character (e.g., higher packet rate or aggregate bit rate) from that described

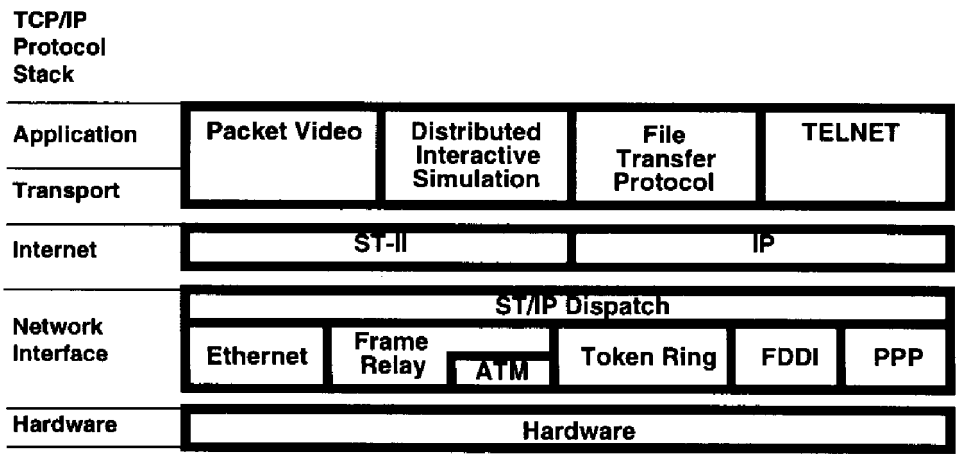

Figure 4. The ST-II protocol is an Internet layer protocol. Implementations exist running over several Network Interface layer protocols including Ethernet, Token Ring, Frame Relay/ATM and several proprietary interfaces.

in the initial reservation request (Figure 5). All of the packets transmitted in a given stream follow the same route to the destination(s) as established at stream setup time.

The packets arrive at the destination(s) in sequence and with fairly uniform delay. (Strict management of the per packet end-to-end delay is supported by the protocol, but not by the existing implementation of the protocol in the T/20 IPR.) In multicast streams, packet replication required to transmit duplicate packets on disjoint network links to reach independent destinations does not occur until the point at which the

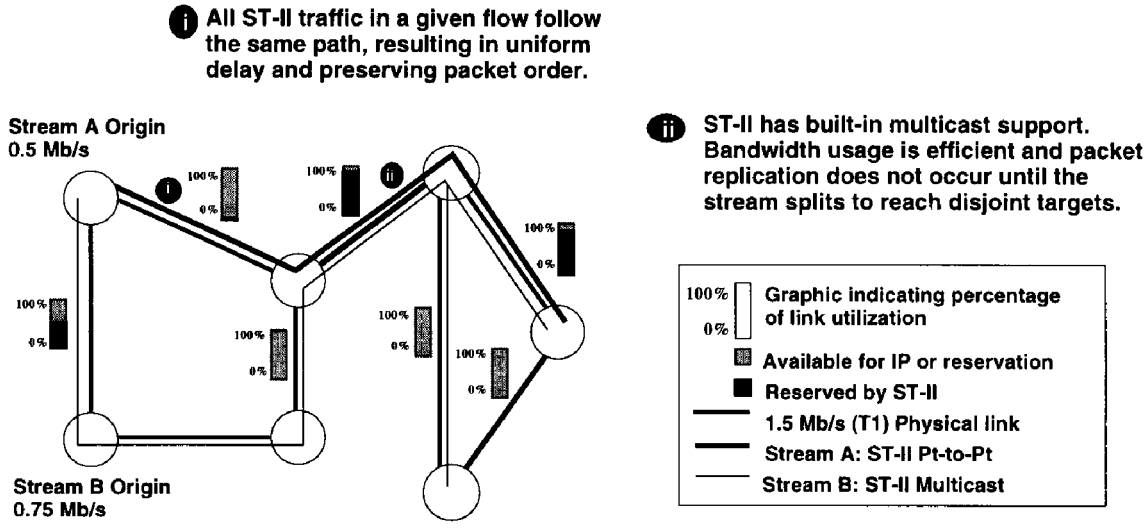

Figure 5. Schematic diagram of an IP/ST internet (circles indicate internet packet routers). ST-II is connection oriented, providing service guarantees, point-to-point and multicast service as well as fast packet forwarding ST-II reserves network resources ahead of time, thereby guaranteeing reliable data transmission.

stream diverges Thus, multicast connections make efficient use of available network resources. The ST-II traffic guarantee continues to be good even in the presence of network congestion which may cause IP traffic flowing through the same routers at the same time to be dropped.

In addition to the requirement for guaranteed QoS, many sites on the DSI have a requirement for sending and receiving classified information over the internet. Communication of classified information over unclassified networks like the DSI can occur if encryption services are provided at the interface between classified and unclassified network components. On the DSI, NSA-approved encryption mechanisms are supported by Motorola Network Encryption Systems (NES).

While the NESes provide an elegant solution to the problem of communicating classified information between classified sites over an unclassified internet, they presented DSI designers with two problems. Firstly, throughput characteristics of the NES limit traffic to less than 200packets/second and 700KBits/second. Secondly, the NES does not support the ST-II resource reservation protocol. Consequently, QoS guarantees could break down whenever there are NESes in the path from source to destination. Both of these problems were overcome by implementation of application software on BBN's T/20 IPRs.

Two application packages were developed to address the problems introduced by the NESes in the DSI. To overcome performance bottlenecks, an End-to-End encryption Interface, running on the T/20s in the classified environment, distributes traffic load over several NESes running in parallel. Thus, additional throughput can be supported by adding NESes to the system. To provide QoS guarantees over paths containing NESes an ST Encapsulation Program (STEP) was developed to run on T/20s in the unclassified environment. The STEP monitors traffic flows between classified sites and automatically establishes ST connections when throughput exceeds a preset threshold.

There are currently 120 participating sites connected to the DSI. These sites span Europe, the United States and Asia. The wide-band backbone supports aggregate traffic rates (summed over simultaneous conferences, simulation exercises, etc.) of up to 3Mbits/second. There are typically two or three multi-site video teleconferences occurring at any given time and, on average, about ten conferences a day. Typical video conferences run at 128KBits/second.

The DSI supports several DIS exercises per year. Exercises involving hundreds of simulators have occurred. Table 1 presents characteristics and measured rates for several of these. As the figures in Table 1 indicate, DIS exercises today are already

within an order of magnitude of saturating the 2xT1 (3MBits/second) throughput capabilities of the DSI backbone. With the introduction of even a modest number of new simulators or simultaneous use of the network for multiple VTCs and simulation exercises, the network will become overloaded. For this reason, ARPA is sponsoring research into ways of scaling up simulation exercises without a commensurate scaling up of the cost of maintaining the network. This research effort includes changes to the DIS protocol to reduce traffic requirements in exercises with large numbers of simulators (10,000-100,000), development of filtering algorithms and exploration of emerging network technology. For example, ARPA is supporting research into the use of ATM as a scalable network architecture for DIS. Research into alternative forms of resource reservation and emerging multicast routing mechanisms is also being conducted.

Table 1. Characteristics and observed traffic rates for several DIS exercises supported by the Defense Simulation Internet [4]

Exercise	A.	B.	C.
Sites	31	13	4
Simulators	210	16	300
Total PDUs	131,000	16,000	850,000
Average Throughput (Bytes/sec)	14,000	6,000	100,000
Peak Throughput (Bytes/sec)	40,000	10,000	290,000
Average Packets Rate (Packets/sec)	70	15	40

DSI TECHNOLOGY FOR THE TELEMETRY RANGE

The DSI and the technologies underlying it are relevant to range operations at two levels. At the first level the DSI can provide the link needed for telemetry ranges and hardware-in-the-loop simulations to communicate and interoperate with interactive simulations at other sites. The DSI provides both the technology and the interconnection to the existing DIS community for this type of integration to occur.

As a second possibility, the DSI could be used by a telemetry range as a reliable mechanism for distributing real-time test data to implement remote monitoring at one or more other ranges or lab or contractor sites. Users need not be limited to using the DSI to supply this capability. The same technology can be deployed in smaller scale, dedicated networks. These networks would be dual use: Real-time data would be transmitted reliably during tests; IP would be transmitted on a not-to-interfere basis. When tests are not in progress, users would see normal response times for file transfers, telnet sessions, etc. During tests, IP packets might be dropped with some

frequency, but the reliability mechanisms built into most IP applications would ensure robust operation at slightly reduced levels of response and performance

In addition, the unique technology that has been developed for the DSI to handle classified communications over an unclassified network will also be of value to the range community. This same technology could be used to support distribution of classified range data in real time to support the implementation of a "virtual range". The functions of test monitoring, generation of quick-look reports and data analysis and archival could be distributed to sites where hardware or personnel were available to perform required functions, thus reducing costs by making more efficient use of existing assets.

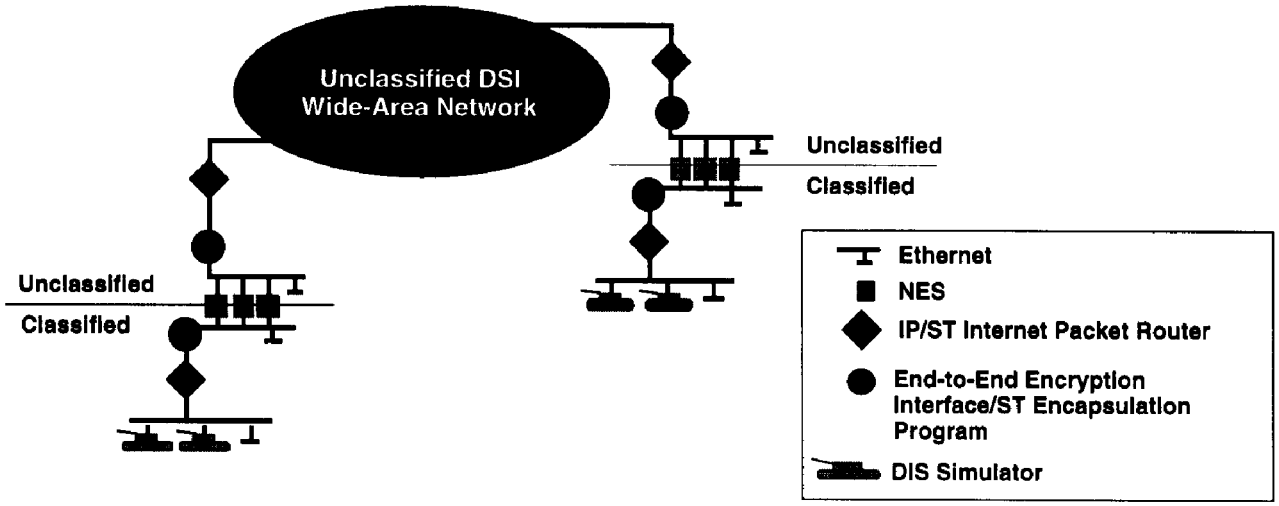

Figure 6. End-to-end encryption devices permit transmission of encrypted classified data packets over an unclassified WAN.

CONCLUSIONS

Telemetry Range operations already involve integration with Distributed Interactive Simulations as well as limited range-to-range interconnection. Introduction of advanced internetworking technology will result in greater range-to-range interconnection to support data sharing, shared use of fixed assets and integration and coordination of tests occurring simultaneously at multiple ranges. These range activities will require: wide-area internetworking; transparent mechanisms for exchanging classified data; and packet-switched network support with Quality-of-Service guarantees. These requirements can all be met using existing technology. The Defense Simulation Internet provides a working example of a communications infrastructure which supports these requirements.

REFERENCES

[1] DIS Steering Committee, "The DIS Vision: A Map to the Future of Distributed Simulation", Comment Draft, Institute for Simulation and Training, Orlando, Florida, October, 1993.
[2] IEEE Standard 1278, "Standard for Information Technology Protocols for Distributed Interactive Simulation Applications", March, 1993.
[3] Topolcic, C., "Experimental Internet Stream Protocol: Version 2 (ST-II)", internet RFC 1190, Internetworking Engineering Task Force, October, 1990.
[4] Seeger, J., "Network Oriented Scalability", Talk presented at the Tenth Workshop on DIS, Institute for Simulation and Training, Orlando, Florida, February, 1994.