Delivering IP Applications in a Tactical Communications Network

A white paper by

Ultra Electronics
DNE Technologies

Ultra Electronics-DNE Technologies
50 Barnes Park North
Wallingford, CT USA 06492
(203) 265-7151
sales@ultra-dne.com

Table of Contents

Introduction: The Changing Face of Tactical Network Operations 3

Traffic Management 4

Information Assurance 5

Protocol Acceleration and Data Compression 6

Practical Issues Confronting Application Delivery 7

Complexity of Configuration and Operation 7

Understanding Network Traffic Patterns 7

Product Performance Must Support Network Requirements for Reliable Traffic Management 7

How to Achieve Adequate Information Assurance Safeguards for Converged IP Networks 8

Weighing Alternatives to Assure Application Delivery 8

Layer 2 vs. Layer 3: Addressing Ease of Use and Performance 8

Fragmentation Strategies: Improving Predictability and Reliability 9

Buffering Techniques: Improving Security and Efficiency 10

Implementing TRANSEC: Assuring Information 11

Ultra Electronics' PacketAssure Offering 11

Overview 11

Traffic Management Elements 12

Information Assurance Elements 13

DoD Plans 14

Delivering IP Applications in a Tactical Communications Network

Introduction: The Changing Face of Tactical Network Operations

With legacy, circuit-based networks, many of which are still operational in the DoD today, the greatest challenge for the network operator was identifying an end-to-end circuit path and enough circuits to satisfy a user's requirement. When a circuit was "turned-up" there was no ambiguity about how much data was going to travel on the circuit and what type of data was going to be transmitted.

Routed, Internet Protocol (IP)-based networks - while adding a dynamic, homogeneous network - have introduced significant new complexities to the network operator. Today the operator has to vigilantly monitor application performance and understand how network performance, and possibly congestion, is impacting users. In addition, safeguarding the source and destination information in an IP packet and detecting security breaches require the architecture to adequately address information risks. Finding enough network capacity to satisfy users remains a challenge for the operator.

Quality of Service (QoS) for IP networks has received a lot of attention lately in the trade press. Bit error rate, data latency, minimum data throughput, and data security practices could all be contemplated as practical performance measures for a tactical network. Performance issues indicated by these measures could result in a variety of concerns:

- Poor voice and video quality
- Slow network response
- Difficulty connecting to network resources
- Unwelcome network intrusions

The most important rule for effective network operation and application delivery is that users and operators must agree on the measures to be observed and the service quality to be delivered for each traffic type on an end-to-end basis, where feasible.

Conceptually, there are three network elements the operator can control to optimize application delivery (see Figure 1):

- Traffic Management
- Information Assurance
- Protocol and Data Acceleration.

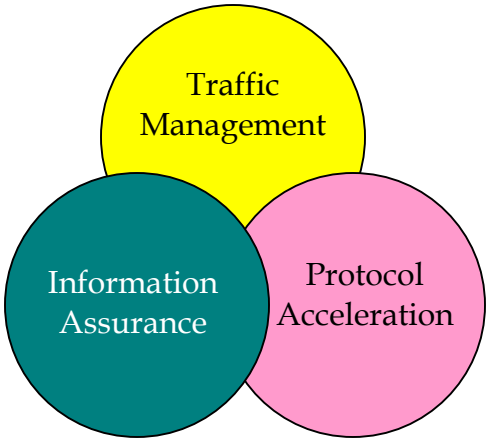

Figure 1. Application Delivery Elements

There are significant inter-dependencies among these elements, such that a decision regarding traffic management may greatly impact the information assurance strategy and vice versa. A clear understanding of which service quality attributes are "Musts" and which are "Negotiable" is required to make the architectural decisions that will result in an effective network.

Traffic Management

Traffic Management, regardless of the protocols or product, includes three functions: **classification**, **precedence or priority**, and **congestion management**.

IP networks have traditionally operated on a "first in – first out" basis with each IP packet receiving equal treatment. The advent of voice and video over IP and interactive Web applications has driven users to demand that some IP packets get differentiated treatment.

Classification is the grouping of IP packets that deserve some special handling by the network. Elements that may define the different classes may be source or destination addresses, service quality designators, physical ports, or the application that generated the packet.

Precedence (priority) describes how the system will treat each class differently as data flows through the network. One class may be guaranteed immediate transmission without waiting in an output queue, while another class may have to wait until all the other classes are idle before being transmitted.

The need for **congestion management** often arises when a Local Area Network (LAN) with gigabits of capacity accesses a Wide Area Network (WAN) through a megabit circuit. Specifically, congestion occurs when the amount of data attempting to access the network exhausts the resources of the network access device and a decision has to

be made about which IP packets get discarded to maintain the integrity of the service quality. Windowed protocols, such as TCP and HTTP, detect lost packets, and after a delay interval will retransmit the packets so that no data is lost.

A decision to discard will arise when a data queue fills to a trigger capacity. Strategies to select which packet gets discarded range from "first-in, first-out" to identifying a packet in the lowest service priority.

Information Assurance

Information Assurance doctrine is controlled by the National Security Agency (NSA) for US military networks. Figure 2 depicts the legacy model for assuring information.

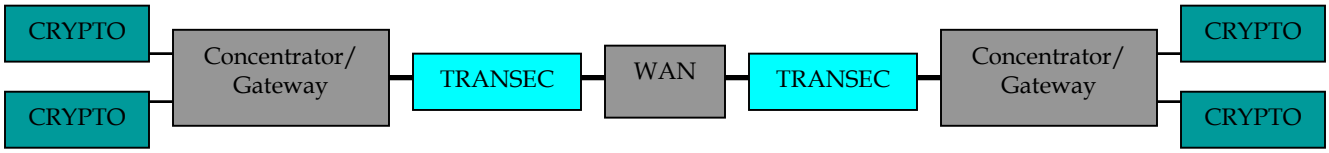

Figure 2. Legacy Information Assurance

A cryptosystem performs end-to-end encryption of a set of data circuits grouped by security classification to prevent non-authorized access to the data. TRANSEC encrypts link data and takes measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis[1]. Committee on National Security Systems (CNSS) policy permits the use of NSA-certified encryption products and commercial AES encryption products[2]. NSA-certified products include government-specified encryption products that support unstructured serial data and IP inline network encryption (INE) products.

Inline encryption uses virtual private network (VPN) technology to secure the information. VPNs take IP packets, encrypt them, and place the secure data in a new IP packet with new source and destination addresses that reflect the INE units, rather than the addresses of the originator and receiver. The address information on VPN packets permits the data to be routed and simplifies operation of the network. The disadvantage of VPNs is that they introduce as much as 20% more overhead into the network and the encryption of the data can deprive the traffic management system of some of the markers desirable for traffic classification. The High Assurance IP Encryption (HAIPE) Guideline describes NSA's recommendation for inline encryption of data.

---

[1] National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999

[2] National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, CNSSP-15 Fact Sheet #1, June 2003

Protocol Acceleration and Data Compression

There are a wide variety of protocol acceleration techniques that can be deployed to improve data throughput and application reliability across IP networks.

For example, web caching is a technique that stores the most recently accessed web files on a server local to the client or the client itself. Execution of web applications makes repetitive use of a key number of files and the web cache eliminates the need to keep retransmitting those files across the WAN to the client.

The TCP protocol maintains end-to-end data reliability and accuracy across the network. TCP is another protocol that introduces high levels of overhead to the network to perform its function. Efficiency can be obtained by consolidating multiple application connections in one TCP session. TCP also monitors data loss and latency to control the speed of the virtual circuit. High-latency mediums, such as satellite, will experience maximum data rates of around 100K bits per second due to TCP control. Spoofing algorithms can be implemented on network access devices to "fool" the network nodes into concluding that a low-latency circuit is present and allow TCP to permit much higher data rates by minimizing latency and reducing the chances of timeouts.

There are also numerous compression techniques available to the network planner. Packet headers, payloads, voice, and video can all be compressed. The improvement in data throughput will be the difference between the data transmission time saved from the data reduction and the time it takes to process the data reduction. The best throughput improvements are achieved on low-speed circuits where the compression can be executed quickly. Voice, video, and ASCII-encoded data streams can experience significant throughput improvement through compression.

Another factor to consider is the Department of Defense's stated objective to transition to IP Version 6 by 2009. The significant increase in the size of the IPV6 packet header over the IPV4 header makes IPV6 a prime candidate for header compression. An additional element of the transition to IPV6 is the strategy for allowing the two protocols to coexist in the network. Dual stack and VPN technologies are often identified as tools for implementing the transition, but there are problems with these approaches. They introduce overhead inefficiencies, security issues and increased operational complexity for network administrators, managers, operators and users alike.
A possibility that will be further examined in this paper is to allow these protocols to coexist at Layer 2 (Ethernet) only.

It is important to note that most of the protocol and data acceleration techniques available need to operate on "plain text" data to be effective. Also, the impact of these tools is lost when the data is encrypted.

It should be noted, in summary, that all these techniques add to the complexity of the network, add to the proprietary nature of a vendors product on either end of the link and make maintenance/operation significantly harder for the typical user in charge of it (installation, training, working, troubleshooting), etc.

Practical Issues Confronting Application Delivery

Complexity of Configuration and Operation

Implementing traffic management schemes on a Layer 3 device, such as an IP router, is a detailed and complex operation. Each port of the router can require 10 to 20 configuration lines to specify the proper classifications, precedence, and discard policies. These configuration sets are dependent on the speeds of the data circuits and require reprogramming if these speeds are changed.

The learning curve for operators is further clouded by proprietary configuration syntax that requires the operator to learn the specifics of each router vendor's control language. This complexity has led some network planners to retreat from the efficiency of converged networks and either diverge the latency-sensitive traffic onto separate network channels or underutilize the network bandwidth available to avoid congestion and latency issues. While both of these steps simplify the configuration of the network and lessen the risk of application degradation, they deviate from the goal of increasing network efficiencies through a converged IP network.

Understanding Network Traffic Patterns

In the introduction to traffic management concepts, it was emphasized that users and network operators need a shared understanding of traffic management policies and service expectations. Inherent in the service expectations is a realistic understanding of the anticipated traffic patterns in the user's network. Communication planners must understand the nature of the applications and devices that the end users will place on the network to predict network traffic patterns and to ensure that the network can produce the environment required by the applications. These patterns can be understood through simulation programs or by directly monitoring similar networks.

Product Performance Must Support Network Requirements for Reliable Traffic Management

Product architectures vary greatly across vendors and the specific characteristics of the architecture will dictate circuit capacity that the traffic management mechanisms can support. Access routers are scoped to support T1/E1 circuits, edge routers with optional support hardware can support broadband rates, and Layer 2 devices can support speeds in between the two (see Table 1).

Table 1. Product Performance

Network Element	Circuit Support
Access Router	T1/E1
Layer 2 Device	T1/E1 - Broadband
Edge Router	Broadband

Factors impacting performance are processor speed, buffer sizes, and frequency with which precedence decisions are made and congestion status is checked. The key issue is that if a product is not scoped correctly for the application, buffers can be overwhelmed and traffic can be dropped. This reinforces the point that users must understand their traffic patterns, as well as their network capacity, to assure end-to-end service reliability.

How to Achieve Adequate Information Assurance Safeguards for Converged IP Networks

Transmitting packet networks over the airwaves presents both familiar and new information assurance risks. Clearly, the risk of data being intercepted requires adequate information security practices. But packet networks, by their very nature, will betray the level of activity on the network by the transmission itself. Since 2003, numerous trials and experiments have studied the benefits and risks of commercial encryption equipment when compared to government-specified encryption. As stated previously, NSA controls the policy decision on this question and applies direction based on product evaluation and the risk and hazard associated with the area of operation, to protect U.S. information systems.

Another product architecture issue is how a router or Layer 2 switch responds to a Denial of Service (DoS) attack. One type of DoS attack bombards an IP address with incoming traffic with the intention that the device will succumb and go offline. Due to buffer management decisions, some routers will crash completely during a DoS attack. Other products have a more robust design and can limit the impact of the attack to one network user service.

Weighing Alternatives to Assure Application Delivery

Layer 2 vs. Layer 3: Addressing Ease of Use and Performance

The "MS PowerPoint® View" of IP networks often reflects a simple router and IP modem tackling all the link and network level technical issues with the IP protocol. While practical for small and simple network problems, this approach bears significant

cost and performance issues as the network scales to support more complex implementations.

A reasonable alternative to consider is to let a specialized Layer 2 switch address the link issues and a router address network issues. A Layer 2 device is defined here as a configurable "switch-like" device that can aggregate Ethernet segments, interface with multiple systems and network elements, and offer traffic management and control tools.

These two classes of devices handle the classification and precedence elements of traffic management in significantly different fashion. Layer 3 devices offer far more parameters from which to create classifications and can support a large number of service classes. As discussed earlier, this capability further increases the complexity involved in configuring the traffic management policy. Layer 2 devices rely on only the physical port and class of service designation to establish service classes. With the reduction in classification options comes a significant reduction in configuration complexity that eases setup and configuration changes. The question is whether the precedence levels available in a Layer 2 device are adequate to service user requirements. For most tactical applications, the focused ability to manage circuit traffic, variable latency-sensitive traffic, and fair weighting of the remaining traffic is adequate for the user base.

The cost and performance attributes of Layer 2 and 3 devices differ with respect to traffic management. Traffic management functions are implemented predominantly in hardware for a Layer 2 device, whereas Layer 3 devices sequence traffic management operations in software with some level of hardware support. Thus, for low-speed, simple applications a small, low-cost access router can successfully manage the traffic. As traffic capacity grows into the multi-megabits per second, the Layer 2 device gains price/performance advantages over the access router. And as link speeds approach fiber data rates, the scalable edge router has an advantage. The key question is which device can meet the traffic management requirement for the mission at the best price with the least weight and operational complexity.

Fragmentation Strategies: Improving Predictability and Reliability

The variable size of IP packets presents a technical challenge when attempting to deliver a constant-bit rate channel over an IP aggregate. The problem arises when a small latency-sensitive packet, like a VOIP packet, is ready for transmission an instant after the transmission of a large, low-priority packet has already begun. Unless the aggregate is extremely high-speed (greater than 8 Mbps), an unacceptable variable latency is introduced by this phenomenon. The solution is to breakup, or fragment, large packets so higher-priority packets can be inserted between the fragmented packets.

The IP protocol has a capability to fragment and reassemble data packets by specifying a Maximum Transmission Unit (MTU). If a data packet is larger than the MTU, the IP protocol will fragment the packet into multiple IP packets. For a router controlled by a general microprocessor, fragmentation can consume significant processor resources. For this reason, higher speed routing devices use a separate processor or programmable gate array to support the fragmentation. Without fragmentation, traffic management will not be reliable and, without hardware support for fragmentation, data throughput will be constrained.

Another variant on fragmentation techniques is whether packets are fragmented into fixed or variable sized packets. Fixed-size packets introduce incremental overhead since padding will be used if the payload does not completely fill a packet. The fixed size of the packets, however, simplifies the processing required for traffic policing, implementing fair weighting policies, and producing meaningful reports to describe how well service levels are maintained.

Selection of fixed or variable packets depends on whether service quality levels or raw data throughput are given greater emphasis.

Buffering Techniques: Improving Security and Efficiency

It is difficult for a network planner to understand exactly how router queuing techniques impact various traffic management scenarios without experimenting directly with the product. Two parameters for the planner to understand are how efficiently different queuing techniques cooperate to use available bandwidth and how much separation is maintained between different classes' buffers.

Most routers offer a queuing technique that will assure that latency-sensitive traffic is delivered in a prompt fashion. Some routers, however, reserve a bandwidth pool to assure the service level is met. With this approach, there is no allowance to release the bandwidth (if the high-priority circuits are idle) without operator intervention. Likewise, all routers support a congestion management technique. It is important to understand, however, how to effectively administer this technique to avoid buffer overflows that will impact other users' traffic.

Related to the congestion management issue is how a device handles a Denial of Service attack. If a router allocates memory resources to these attacks without constraints, the device will often fail. An alternative is to limit the number of memory buffers that can be assigned to a class. And if classes are defined such that different users' traffic are not commingled within a class, the denial of service attack can be contained and the device will remain online.

Implementing TRANSEC: Assuring Information

As mentioned earlier in this paper, users have closely weighed whether to use legacy or commercial encryption devices. The NSA policy for implementing TRANSEC over wireless networks in hazardous areas of operation continues to evolve. Concerns also still exist for using AES encryption products for TRANSEC in hazardous environments. There are COMSEC solutions based on legacy encryption products that are suitable for IP wireless networks.

Legacy serial encryption products can be implemented if the network access point supports unstructured serial data over IP and has the ability to loop plain text to a legacy encryption device and return the cipher text to a port that will wrap the data in an IP packet and direct the flow to the IP wide-area network (see Figure 3). A Layer 2 switching device can manage this problem without introducing excessive latency and consuming significant processor-memory resources.

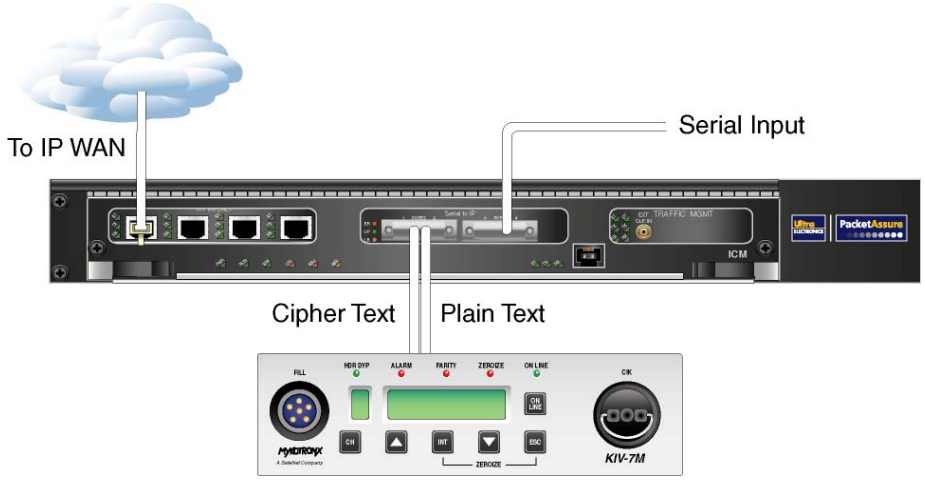

Figure 3. Legacy Encryption Implementation

Ultra Electronics' PacketAssure Offering

Overview

PacketAssure is a switch that operates at the link and Ethernet layers. It complements existing IP router networks by shaping and policing LAN segments before aggregating them onto an Ethernet link with legacy circuit traffic.

Traffic management is implemented by assigning a service classification to each Ethernet port. Classifications include Priority, Variable, and Best-Effort flow rates. A high-speed network processor analyzes the data rates on each configured port and

polices non-conforming IP packets traffic for discard. High service quality can be obtained by permitting users to easily pinpoint the applications subject to discard without complex policy definitions and configuration.

Each PacketAssure interface is modeled as a virtual circuit. Traffic management actions are taken based on the virtual circuit service class configuration or detection of congestion for data accessing the aggregated Ethernet uplink. To overcome variable latency issues, IP data is fragmented into fixed-sized packets and tagged with destination and service class information before being fed into a switch matrix. After switching to the destination interface port, all IP packets are reassembled and PacketAssure tags and service identifiers are removed. The buffering and switching architecture of the PacketAssure keeps the virtual circuit data isolated from other circuits to deliver high information assurance.

Virtual tunnels connect the PacketAssure ingress points to the egress points, while the PacketAssure core functions as a smart bridge to map data between source and destination MAC addresses. The network processor creates and maintains an Ethernet MAC address table that permits the switch matrix to direct traffic only between the originating and destination interface ports.

Traffic Management Elements

Classification

As indicated above, each physical port of the PacketAssure is assigned one of the three service classes: Priority, Variable, or Best-Effort. From the system's Graphical User Interface (GUI), operators assign one to four traffic management parameters per port. Configuration is quick and can be easily modified to accommodate changing requirements.

Precedence

The PacketAssure supports three general service classes: Priority Flow Rate (PFR), Variable Flow Rate (VFR), and Best-Effort Flow Rate (BEFR).

- PFR is the highest priority and will preempt any lower priority traffic. Applications best suited for PFR have predictable bandwidth requirements, like voice over IP or serial data transmission. Applications with sporadic bandwidth requirements may use PFR with the support of a windowed protocol like TCP or HTTP.
- The second priority is VFR and it preempts BEFR traffic. VFR is modeled for applications with a nominal variation in bandwidth requirements like video over IP.
- BEFR is the lowest priority and is modeled for best-effort traffic. BEFR, however, may use all unused bandwidth when PFR and VFR applications are

inactive and each BEFR circuit is guaranteed a minimum data rate. Peak data rates and buffer sizing may be used to give weighting to the BEFR circuits.

Congestion Management

A unique aspect of the PacketAssure is the ability to measure the rate at which data is flowing over a virtual circuit. Each virtual circuit is assigned a peak data rate to facilitate "fair" sharing of bandwidth across circuits. When PFR and VFR circuits exceed their peak data rate, the non-conforming packets are discarded. When BEFR circuits exceed their peak data rate, operators may choose to either discard the non-conforming packets or tag them as non-conforming. If there is no congestion on the egress side of the PacketAssure the non-conforming packets will be transmitted. Otherwise, non-conforming packets will be discarded at the egress point.

Information Assurance Elements

Type 1 Encryption for TRANSEC

Figure 4 illustrates how PacketAssure supports Type 1 encryption over a TRANSEC link. The application depicts three different IP users and a legacy serial data circuit being policed and aggregated by the PacketAssure before framing and switching the data to a serial EIA-530 data port. The serial port is cabled to the plain text side of the encryption unit and the cipher side is cabled to a third serial port on the PacketAssure. The PacketAssure encapsulates the cipher data in IP packets and sends the packets to an IP radio for transmission. This allows for the use of military or commercial radio systems in a secure environment

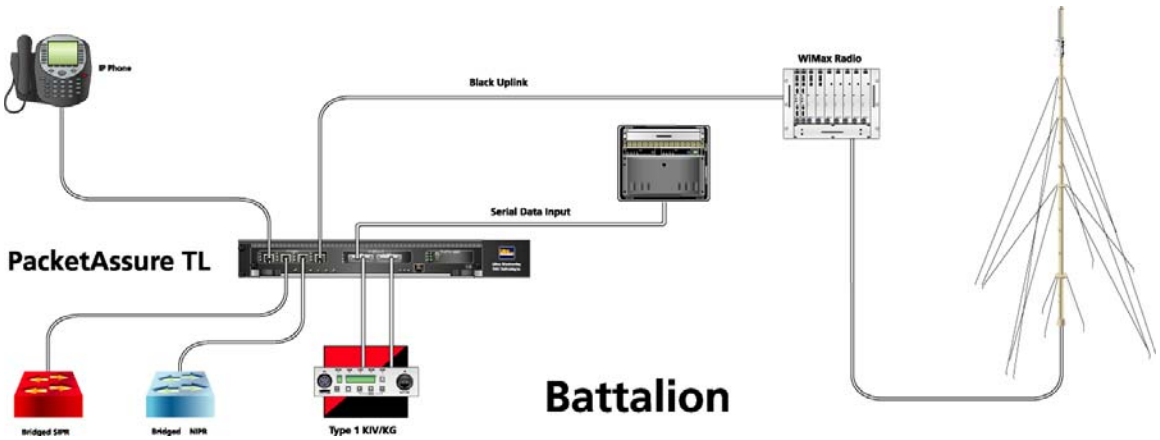

Figure 4. PacketAssure with Type 1 Encryption over TRANSEC

Data Separation

Each data port on the PacketAssure has its own memory buffer assigned to it. Combined with the PacketAssure switch matrix, the system maintains data separation between different user ports without adding the additional overhead of a VPN layer.

PacketAssure Enhances IP-Based Modems

As the DoD has begun to transition to IP-based networking there have been a number of IP-based RF modems introduced to the network. Many of these modems incorporate a small access router within their package. As mentioned earlier in this paper, the processor of a small access router can easily be overwhelmed by the requirements of handling varying packet sizes, making policy decisions based on packet priority and routing traffic onto the WAN as a network scales in size. This can result in significant latency or throughput issues. The PacketAssure offloads this router of the need to make policy decisions and to respond to varying packet sizes, allowing the IP modem to use its processing power to route the traffic efficiently to its intended destination.

DoD Plans

The PacketAssure system was demonstrated as an element in the Flexible Converged Services System during JUICE 2006 at Fort Monmouth. DNE will continue compliance and certification testing with a number of DoD agencies throughout 2007.