



PacketAssure Service Delivery Manager

Simplifying IP Networks with Superior Quality of Service

- Guaranteed Quality for Priority Traffic
- Type 1 TRANSEC Support for Wireless Networks
- Aggregates IP and Legacy Circuits over IP
- Maintains Separation of Data Streams without VPN Overhead
- Concurrent IPV4 and IPV6 Support

Overview

Speed, mobility, and availability drive the rapid evolution of the modern military network. An expanding user base needs access to key applications from one network port, while connecting to the network over radio, satellite, or wire line. Internet Protocol (IP) is at the center of this transformation and is replacing circuit networks to support greater access and mobility. The escalating demand for communication services is driving networks to integrate optics and high-speed radio to address bandwidth requirements.

Even with the rapid migration to IP broadband technologies, technical challenges still abound for extending converged communications to the remote war fighter. Chronic congestion issues at the access points of the network jeopardize time-critical communications to the war fighter, increasing the risk that key communications may be lost or delayed. The security issues surrounding how classified and non-classified information coexist on the IP network have led to introduction of virtual private networks (VPNs) that degrade data throughput, increase equipment inventory, and present complexity to the network operator.

The PacketAssure Service Delivery Manager addresses these issues by preserving the quality of voice and video communications over congestion-prone IP network links as reliably as legacy, time-division multiplexed solutions while supporting the data throughput efficiencies of dynamic packet networks. In addition, PacketAssure will maintain separation of data between networks that eliminate the need for VPNs, and free in-line encryption units to secure payloads only. PacketAssure eases the transition to IP Network-Centric networks with legacy circuit interfaces, such as EIA-530, which encapsulate data in IP packets and applies a priority to assure reliable operation of circuit devices over the IP Network.

PacketAssure

Ultra
ELECTRONICS

Overview

The PacketAssure Service Delivery Management Platform operates at the link and Ethernet layers, complementing 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 network processor analyzes the data rates on each configured port and controls data throughput by identifying packets that exceed a peak data rate and tag them for retransmission. High service quality can be obtained by permitting users to pinpoint the applications subject to discard without complex policy definitions and configuration.

The PacketAssure Core

The key elements of the PacketAssure core are a network and host processor. The network processor has a separate data buffer associated with each PacketAssure interface port. Each interface is modeled as a virtual circuit and traffic management decisions are made based on the configured policy for each virtual circuit and 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 all fragmentation overheads are removed.

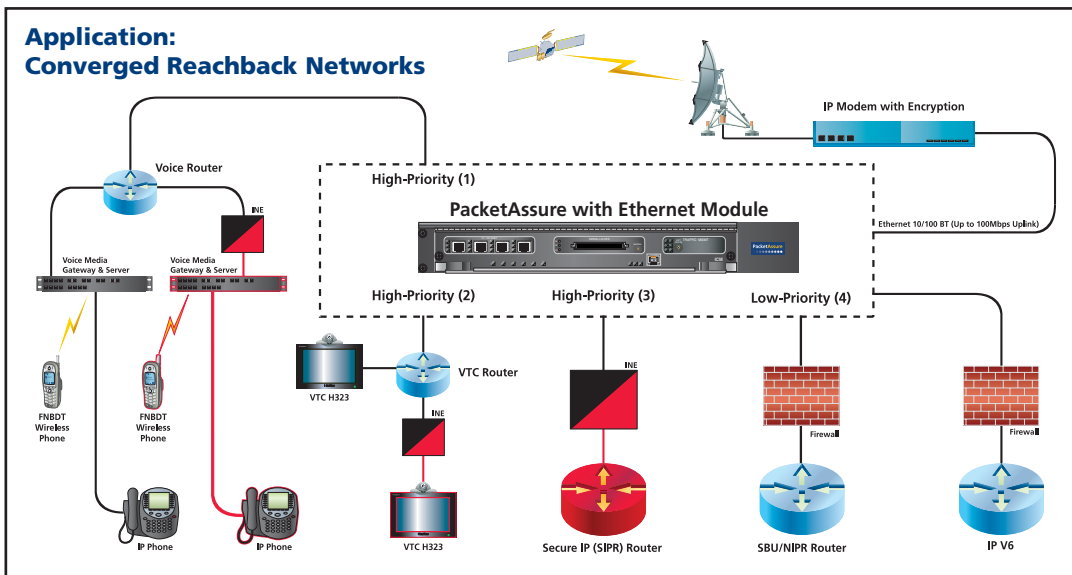
The buffering and switching architecture of PacketAssure keeps the virtual circuit data isolated to deliver high information assurance.

Virtual circuits connect the ingress points of PacketAssure to the egress points, making PacketAssure's core function as a smart bridge to map data between source and destination 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.

The host processor controls all operator interfaces and manages all configuration elements. The operator interface includes a SNMP agent that supports monitoring and control of PacketAssure.

Traffic Management

The PacketAssure Service Delivery Manager 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 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.



Most reachback circuits today are still based on time-division multiplexed (TDM) technology. Replacing TDM technology with IP packet technology expands the communication link from a simple point-to-point connection to an access point to the greater defense network. In addition packet technology provides better bandwidth sharing and efficiency. The PacketAssure Service Delivery Manager supports the move to IP by assuring the critical command and control information is not degraded during congestion periods. In addition, PacketAssure can transport IPV4 and IPV6 traffic without a dual stack and the associated information assurance issues.

The application above depicts IP applications receiving a traffic management priority by routing the application to a specific PacketAssure port. The Priority Flow Rate can assure that VOIP and video traffic maintains quality over the converged satellite link.

A unique aspect of 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. Packets that exceed the peak data rate are candidates for retransmission in event of data congestion. The VFR class of service also permits administrators to specify a sustained data rate and maximum burst size for VFR circuits. PacketAssure will assure that all VFR packets conforming to the sustained data rate are delivered to the network. If there is a period where the VFR circuit uses less than the sustained data rate and there is bandwidth available not being used by another PFR or VFR circuit, the VFR circuit may burst up to the peak data rate until the maximum burst size is exhausted.

In addition to service classification and data rates, administrators may select a buffer size associated with each virtual circuit in the system. In effect, increasing the buffer size improves the delivery priority for a connection by accepting more latency in the circuit to avoid discarding of data during brief congestion periods. Configuring buffer sizes allows traffic management of multiple BEFR circuits to be differentiated.

Model Descriptions

The PacketAssure Service Delivery Management Platform is available in the TL and EX models. Both models support AC power and are rackmountable. The TL model offers two interface slots and includes a Traffic Management Processor and a built-in Ethernet management port. The TL model supports up to 8 ports of Ethernet or Serial data.

The EX model offers redundant AC power supplies, six interface slots, and up to three Traffic Management Processors. All interface modules are interchangeable between the TL and EX models. The EX model includes System Utility Modules (SUMs, ordered separately) that provide for management and timing functions, as well as an alarm relay to make operators aware of system alarms. SUMs may be configured redundantly and can be ordered with or without a Stratum-3 timing source for network timing.

Interface Modules

Four-Port Ethernet Interface: The interface includes four 10/100T Ethernet ports that can be configured independently to support IPV4 or IPV6 traffic. Each port can be assigned a unique service class and traffic management parameters.

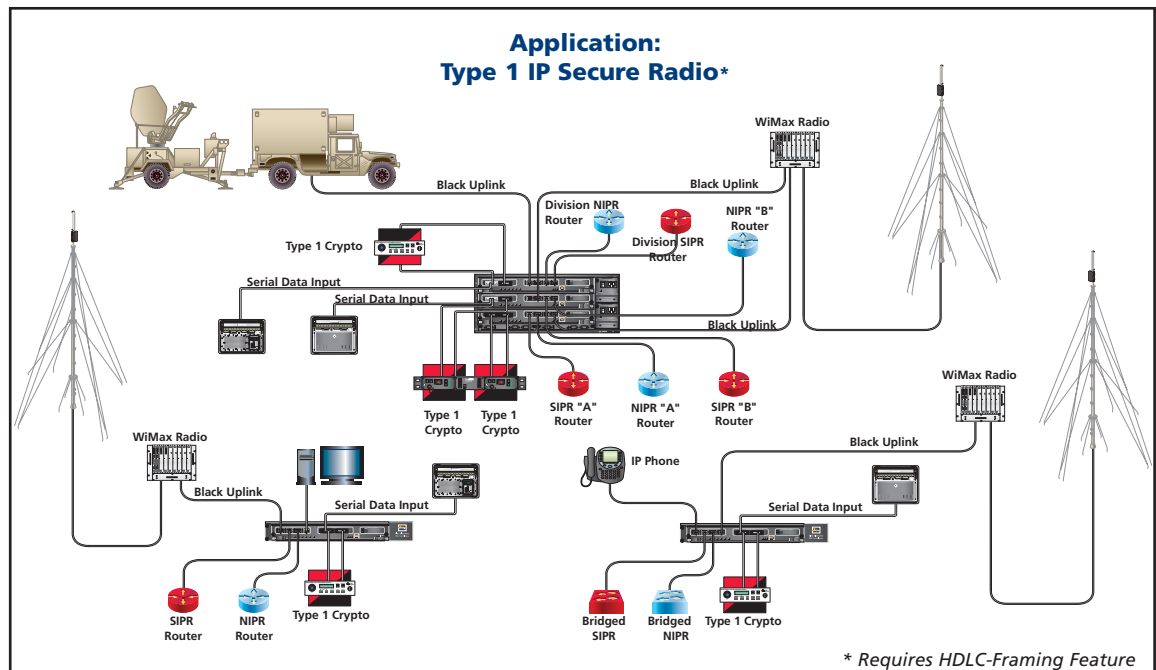
Serial to IP Interface: The interface includes four EIA 530 synchronous data ports that either encapsulate unstructured data into IP packets (Normal Mode) or pass an Ethernet stream through HDLC framing (Framed Mode). The interface can receive timing from a station clock, an external transmit clock, or the PacketAssure's internal clock.

Operation of port control may be independently configured to be disabled, handshake as specified by the EIA 530 standard, or the state of the local DTR lead may be transferred across the network to the remote DSR lead for "Push to Talk"-like signaling across the network. Separate from control lead configuration, the RTS lead can be configured to signal PacketAssure to enable or disable Normal Mode port data transmission, dynamically releasing bandwidth to other applications when the port is not in use. While in Framed Mode, the interface will detect loss of framing on the port and reset encryption equipment as required.

Each Serial to IP port has a unique MAC address and the user configures the IP address, subnet mask, and IPV4 TOS bits. The IP packet payload size is user-configurable and constrained by the data rate selected.

Management

The PacketAssure Service Delivery Manager may be operated from a serial console port or either a telnet or http-based interface that runs on an integrated, Ethernet management port. In addition, a SNMP client and Management Information Block (MIB) are available to monitor PacketAssure operation from a Network Manager.



Wireless technology is being deployed to bring the perimeter of the network closer to the warfighter. Network implementers must answer the challenge of supporting multiple applications over a wireless link and assuring that the data is secure. The PacketAssure Service Delivery Manager adds value to wireless networks by aggregating IP and legacy data streams with proper quality of service considerations, switching the aggregate through a Type 1 encryption unit, and encapsulating the black data in IP packets before sending the data to the radio.

The diagram above depicts two IP networks attached to two Ethernet ports and a serial data input attached to a Serial to IP port. PacketAssure shapes the data and switches an HDLC stream out to a third Serial to IP port, then into a Type 1 crypto. The BLACK data is returned to the a Serial to IP port, placed in IP packets and switched to an Ethernet port for radio transmission.

	PacketAssure TL	PacketAssure EX
Interface Control Unit (ICU)	Each ICU supports one Traffic Management Interface and two Additional Interfaces One per TL unit	Three per EX unit <i>Population of Second and Third Traffic Management Interface is Optional</i>
Maximum Clients	2036 Nodes (One ICU only)	2036 Nodes per ICU, for a Maximum of 6108 Nodes (Three ICUs Required)
Control Ports	Serial: DB-9F. Ethernet: RJ-48.	
Traffic Management Processor		
Number of Aggregates	Two per processor; one processor per TL unit	Two per processor; up to three processors per EX unit
Total Throughput	11 Mbps per processor	11 Mbps per processor
Ethernet 10/100T 4-Port Interface	RJ-48, one per unit (4 ports total)	RJ-48, up to three per unit (twelve ports total)
Serial-to-IP 4-Port Interface (SIPI)	One per unit	Up to five per unit
Data Rates <i>Normal Mode:</i>	75, 600, 2400, 4800, 9600, 16000, 19200, 32000, 64000, 128000, 256000, 384000, 512000, 768000, 1024000, 1536000, 2048000, 3072000, 4096000, 4608000, 5120000, 6144000, 8192000. (bits per second) Total data throughput: 16384000 bps per interface.	
<i>Framed Mode:</i>	64000, 128000, 256000, 384000, 512000, 768000, 1024000, 1536000, 2048000, 3072000, 4096000, 4608000, 5120000, 6144000. (bits per second) Total data throughput: 16384000 bps per interface.	
Data Format	Unstructured or HDLC-framed Ethernet	
Electrical Interface	EIA-530, requiring breakout cables	
Physical Ports	Two DB-60P connectors per interface	
Dynamic Bandwidth	Activated by RTS control lead (Normal Mode)	
Power	AC-Power Supply Unit (PSU): 90 to 132 VAC, or 180 to 264 VAC, 47-63 Hz, Fan Cooled Autosensing 100W PSU	Two redundant 300W power supplies, Field replaceable
Dimensions	17.5" W x 12.0" D x 2.35" H 13.5 lbs fully loaded	17.5" W x 12.0" D x 7.0" H 34.0 lbs fully loaded
Environmental	0 ^o to 50 ^o C Operating, -40 ^o to 70 ^o C Storage, 5 to 95% Humidity (non-condensing), -500ft to 10,000ft (-152m to 3048m)	
System Clocking	Clock Sources: Internal Reference Oscillator, recovered from user-specified interface or station clock.	

PacketAssure is Patent Pending.



Ultra Electronics
DNE TECHNOLOGIES
50 Barnes Park North
Wallingford CT USA 06492
Tel: (203) 265-7151 Toll Free: (800) 370-4485
Fax: (203) 265-9101 info@ultra-dne.com
www.ultra-dne.com

Ultra Electronics DNE Technologies reserves the right to change these specifications without prior notice.

© 2008 Ultra Electronics DNE Technologies Printed in USA