Ultra ELECTRONICS

DNE TECHNOLOGIES

PacketAssure iQ Series

Application Guide

February 2011

This document is not export controlled.

1. Introduction

With so many demands on today's networks the warfighter is confronted with the need to prioritize the informational lifeline. Whether it is in deployed tactical environments with limited telecommunications infrastructure or on base where streaming visual intelligence from an unmanned aircraft is battling two video teleconferences and 150 soldiers watching a sporting event online for available bandwidth, Ultra DNE has created the PacketAssure iQ Service Delivery Manager to ensure that the critical data gets through.

The PacketAssure iQ Series from Ultra DNE is a family of high-performance switching systems offering a unique traffic management solution that assures delivery of Real Time Services over a communications infrastructure. PacketAssure has demonstrated its ability to enhance or replace IP Convergence Routers, increase call completion rates, simplify router configurations, decrease training requirements and make IP communications as reliable as the TDM networks that they are replacing.

Featuring a powerful Web 2.0-style Graphical User Interface (GUI) the PacketAssure iQ Series allows network planners to quickly achieve the benefits of Unified Communications with the people and platforms that are in place today with minimal training.

2. PacketAssure iQ Overview

The PacketAssure iQ is a Layer 2 convergence device designed to simplify the QoS Policy implementation of a network and provide management of the bandwidth entering or exiting a location by offloading convergence routers of the prioritization decision making, cross connection and protocol adaptation functionality. This results in more predictable traffic patterns, allows users to retain less expensive routers and decreases the IP training requirements of the network.

The PacketAssure iQ eliminates the need for class and policy maps on WAN facing routers. This greatly simplifies the configuration of these routers and diminishes the need for processing power in the convergence router.

The PacketAssure iQ 1000 is currently shipping and is a 1 RU, 18GB switch with up to 18 Ethernet or serial data ports. The chassis offers up to three module ports. The serial module can be used to encapsulate serial data traffic in IP at rates up to 20MB per port or as a serial aggregate for connection to serial modems such as FDMA satellite modems at rates up to 20MB.

The PacketAssure iQ 4000 is currently in development and is a 4RU, 66GB switch with up to 66 Ethernet or serial data ports. This chassis adds redundant power and packet switching capability. The interface modules are interchangeable between the two models.

3. Applications

The PacketAssure iQ is a versatile network appliance that can be used in a wide variety of applications from a simple IP multiplexer to a complex QoS policy administrator for multi-aggregated multi-enclave coalition networks.

3.1 IP Multiplexer

The PacketAssure iQ can be used to replace legacy ATM or TDM multiplexers. Serial and Ethernet streams can be combined onto serial (up to 20MB) or Ethernet aggregates (Up to 1GB). The device can migrate from serial to IP as the network migrates.

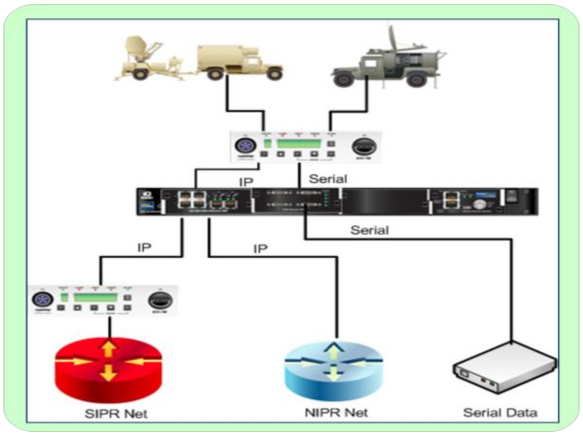

Figure 1 – IP Multiplexer

3.2 DSCP Gateway

As networks migrate to nearly everything over IP, the need to prioritize traffic across the converged network increases. Applications that operate within a converged network may have differing needs in terms of bandwidth, latency tolerance and jitter tolerance. Most networks that include Real Time Services make use of the DiffServ Code Point (DSCP) field in the IP header to identify application types and to offer prioritization to traffic. The challenge is that organizations are developing their own DSCP tables so that if traffic needs to cross from one domain to another, the network devices may not understand the traffic needs of the packets that have been sent. The PacketAssure iQ can easily provide gateway services and translate between two different DSCP domains at the interface point between the networks.

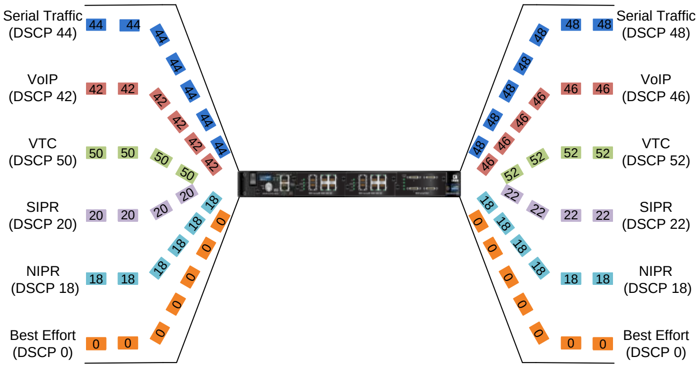

Figure 2 – DSCP Gateway

3.3 Unified Capabilities Integrator

Real Time Services (RTS) in IP networks are being bundled under the common term of Unified Capabilities (UC). Protocols such as Assured Services –Session Initiated Protocol (AS-SIP) provide control within particular domains such as voice as to how much of a limited asset is allowed to open connections on the network. DSCP values are used to determine the precedence of traffic competing for limited transmission bandwidth. The challenge is that as the UC enclave is introduced to a command post, the non-UC applications will now be considered Best Effort traffic if they do not have the proper DSCP codes. The PacketAssure can use almost any information available in the IP header such as MAC address, IP address or application port to classify traffic and then apply a DSCP value to that traffic. In this manner, non-UC traffic is now given adequate prioritization by devices in the network.

A related application is that even with protocols such as AS-SIP and DSCP values, UC traffic may still be impacted in a congested network. If a UC voice device such as a Local Session Controller (LSC) is programmed to expect that it has sufficient bandwidth for five phone calls but the customer edge router is flooded with non-UC traffic, the UC traffic may be impacted. The LSC will continue to allow up to five simultaneous calls but the customer edge router may not be allocating enough bandwidth for these calls. This will result in degraded and dropped phone calls. The PacketAssure iQ can provide a Committed Information Rate (CIR) for the UC traffic or any other designated traffic and will police the network to ensure that this bandwidth is available when needed.

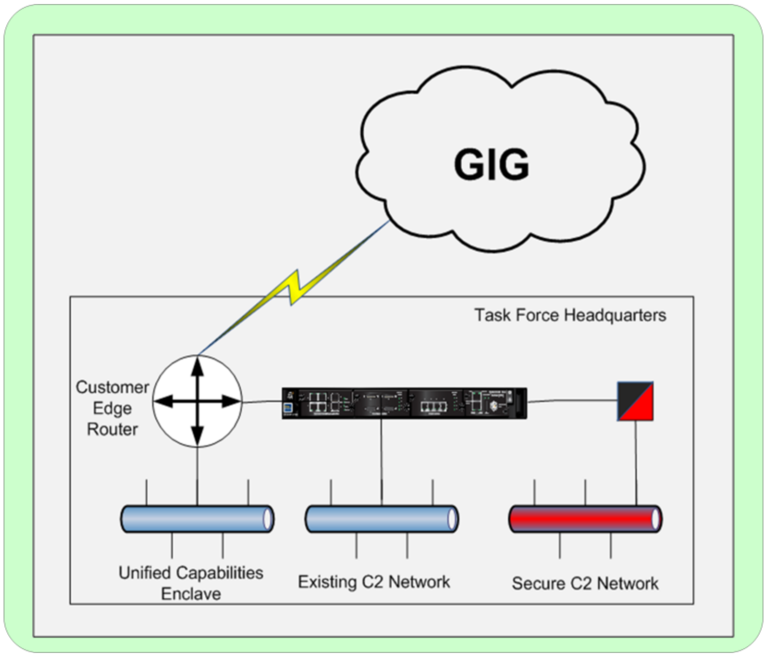

Figure 3 – Unified Capabilities Integrator

3.4 Fine Grained QoS for C4I and CS Networks

The goal of most modern IP networks is to migrate as many applications, enclaves and previously stove-piped systems into a common network infrastructure. This will result in the mixture of C4I traffic, Combat Systems (CS) traffic such as sensor data and fire missions and potentially Morale and Welfare applications for deployed service members. The challenge of such networks is that CS traffic must be transmitted unimpeded and cannot be a statistical calculation that the traffic “should” get across a congested link. The PacketAssure iQ switches, classifies, meters, marks and traffic manages all of the flows that transverse the device. Traffic flows can be classified by almost any Boolean combination of information found in an IP header. Policies are then applied to each flow of traffic as designed by the network administrator. With over 1000 possible policies and classifiers, the limits of how detailed a network can be managed are virtually limitless. The PacketAssure iQ will ensure that the critical applications get across the network when they are transmitted and that all available bandwidth can be shared when not needed by the high priority traffic.

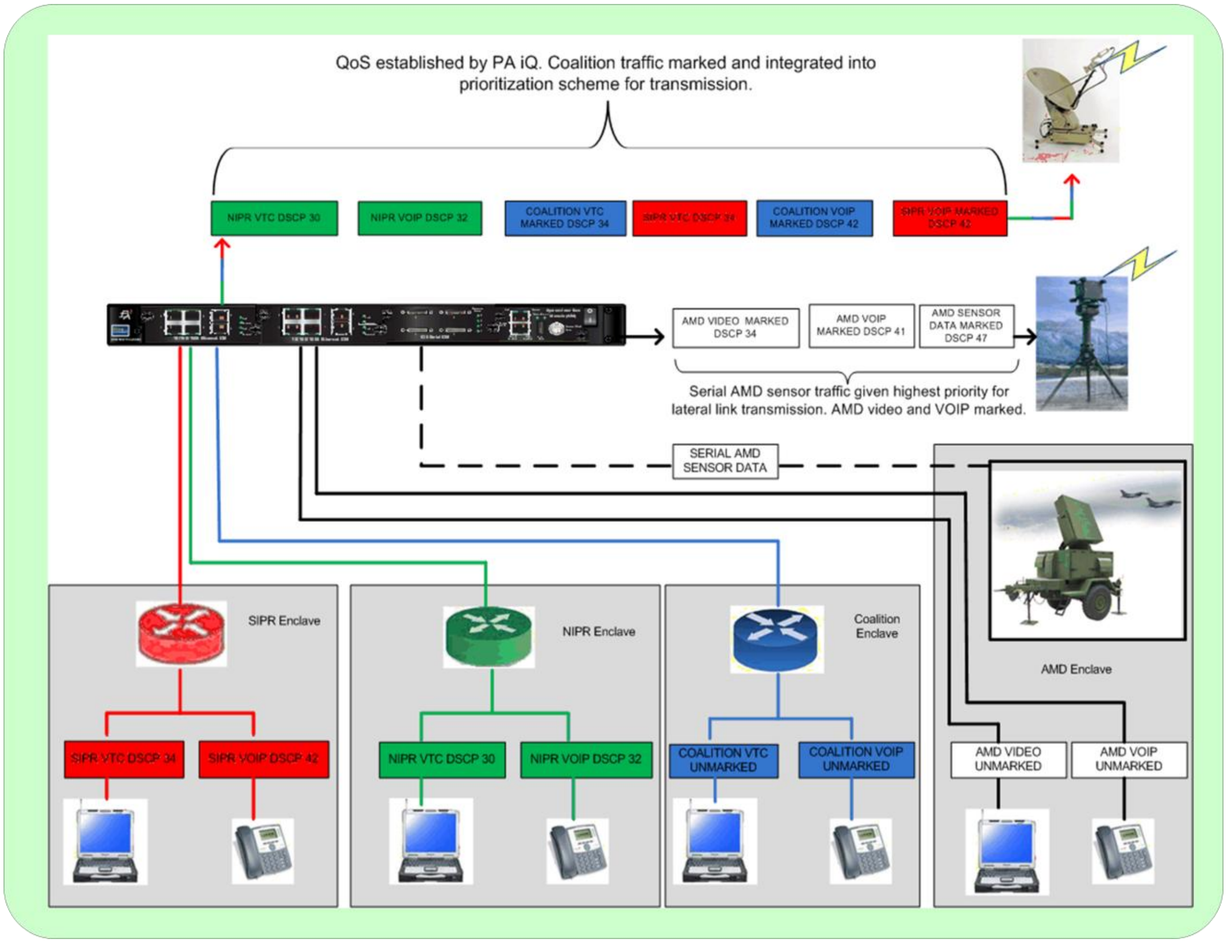

Figure 4 – Fine Grained QoS for C4I and CS Networks

3.5 Field Adaptation to Mission Changes

Military organizations are unique from the commercial world in that they and their networks often face rapid changes in missions and are often under assault from an adversary. As a mission rapidly changes or a communications asset is damaged or destroyed, military communicators must be able to adjust the network to operate in what could be a significantly different environment. Priorities for applications may change depending on the severity of the change in mission. The change to the QoS policies to meet the new scenario needs to be easy and quick to implement. IP Experts may not be available to reconfigure class maps and policy maps on the routers. If an error is made in these changes, the network could crash. The PacketAssure iQ is designed so that the wizards in the GUI can be used to define templates and profiles that can be loaded into the box prior to a mission. If a change occurs, a minimally trained operator can invoke a new template or profile to match the mission within in several commands of the GUI. When the templates and profiles are created, the GUI validates the settings to ensure that the template is usable. In some networks, the changes can be programmed to occur automatically based on a schedule or particular changes in the network performance.

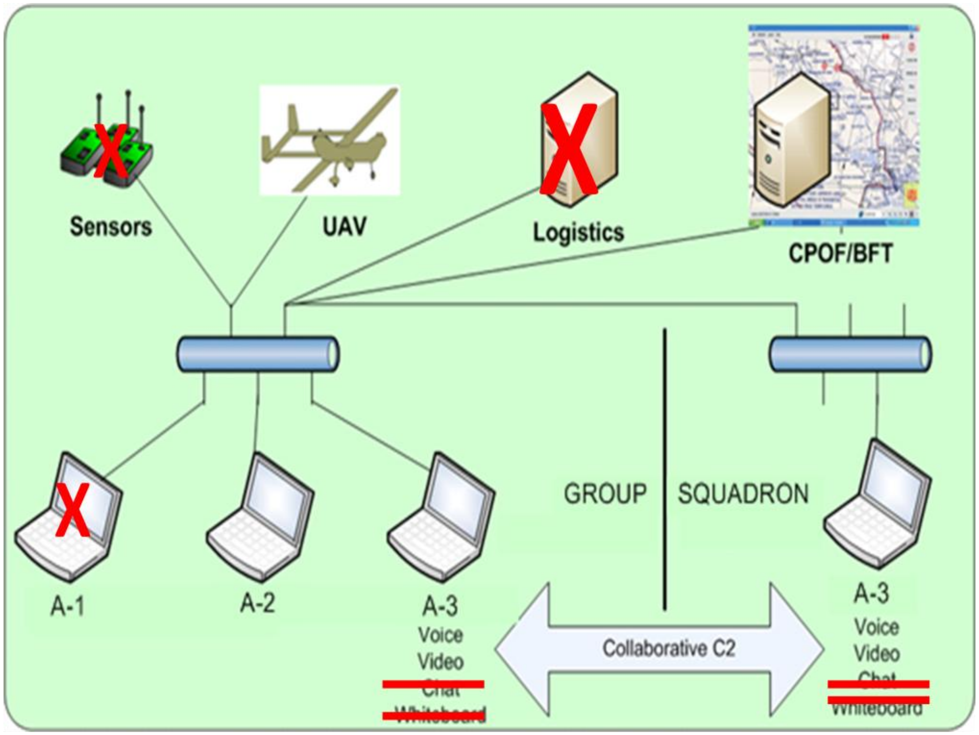

Figure 5 – Field Adaptation to Mission Changes

3.6 Simplification of Lower Echelon Networks

The largest cost for most IP-based networks is the training that is required for the operators of the network. When many networks look to migrate from legacy TDM or ATM technologies, they replace the multiplexers and switches with routers. The PacketAssure iQ offers the ability to deploy an intelligent switch down at lower tier echelons. These switches pull services from other locations in the same manner that voice long local circuits operate. This diminishes the amount of equipment and training that is needed in these smaller units.

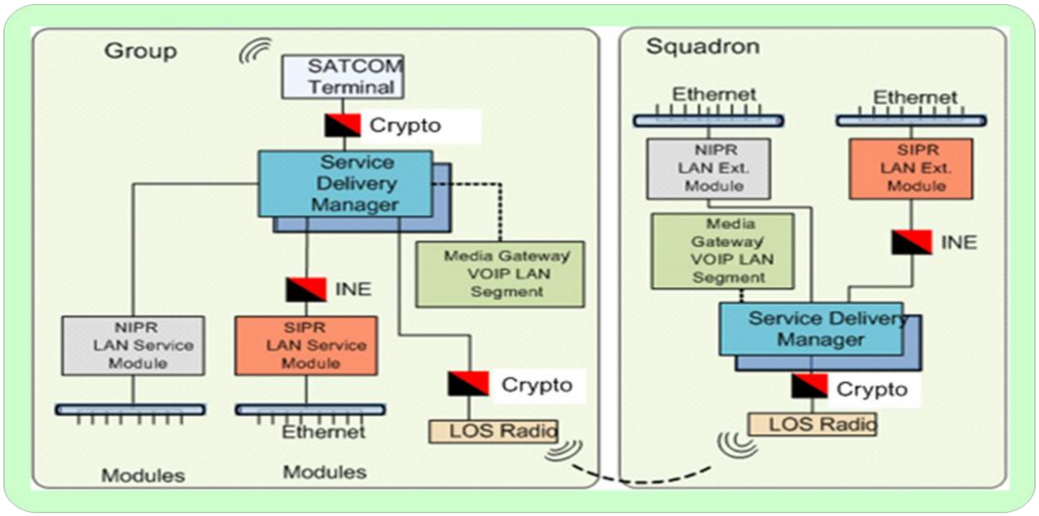

Figure 6 – Simplification of Lower Echelon Networks

3.7 Strategic Governor

The proliferation of social networking sites and the increased use of these sites is placing increasing burdens on the bandwidth requirements of strategic networks. While some advocate for blocking access to such bandwidth intensive sites, many leaders are seeing these sites as a necessary part of the lives of many younger service members and that these sites offer tremendous morale and welfare benefits as well as potential recruiting benefits to the services. As the demand for these services grow, the risk for congestion with strategic applications grows unless more bandwidth is acquired or the strategic applications are given an easy to use precedence mechanism. The PacketAssure iQ can ensure that strategic applications are given priority at network service centers and that if necessary the access to social networking sites is limited to the degree necessary to allow the strategic traffic to enter the network.

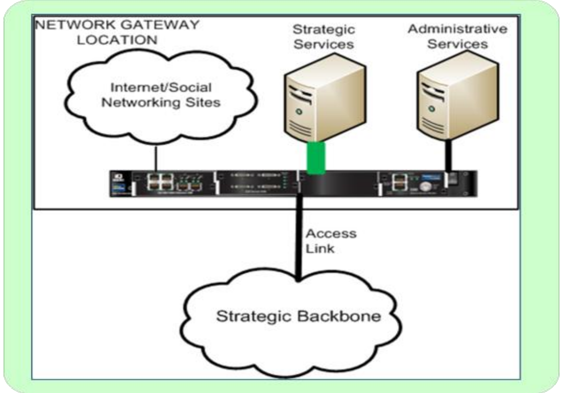

Figure 7 – Strategic Network Governor

3.8 TRANSEC Enabler

Because network devices make use of information such as DSCP values to make prioritization decisions, Transmission Security (TRANSEC) standards have been modified to allow for DSCP values to be copied over from packets in the Plain Text (PT) side of an encryptor to the Cypher Text (CT) side of the encryptor. This allows for convergence devices to still offer QoS in the network. As the reachback link is often the most likely congested link in a network, it is paramount that the traffic receives proper QoS treatment at this point. However, the backbone of a network is far less likely to be congested lessening the need for QoS. If a security official is concerned about transmitting DSCP values across the WAN, the PacketAssure can accept the DSCP values from subtending enclaves and then null the DSCP field after the traffic has been prioritized on the egress port. The aggregate can be serial or Ethernet.

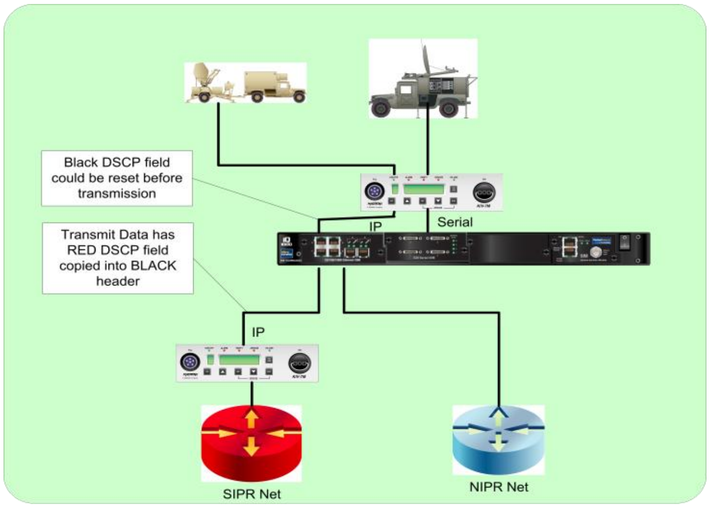
Black DSCP field could be reset before transmission
Transmit Data has RED DSCP field copied into BLACK header
IP
Serial
IP
SIPR Net
NIPR Net

Figure 8 – TRANSEC Enabler

4. Descriptive Videos and Specifications

Additional information to include instructional videos, data sheets and additional application information regarding the PacketAssure iQ can be found at www.packetassure.com.