DNE TECHNOLOGIES

White Paper

What is a Service Delivery Manager?

19 October 2009

To understand the role of a Service Delivery Manager (SDM), it is important to first describe the concept of 'Service Delivery'. Every application running on an IP network has service delivery requirements. Voice and video applications require low latency and jitter; collaborative applications require low latency but can tolerate some jitter, while file transfers and email are largely immune to latency and jitter concerns. Additionally, key users may require preferential treatment over that offered to normal users, regardless of the applications involved. Generally speaking, Service Delivery refers to the ability to allocate network resources to communications services based on user requirements. More specifically, Service Delivery improves users' productivity and capability by improving the quality of their communications experience – be it voice, video, data or all three – over constrained transmission facilities, in a unified manner.

With that said, a Service Delivery Manager combines high performance hardware with intelligent software to create, administer, prioritize and manage converged IP and telecom services in a predictable manner. Users benefit from an integrated communications experience, enabled by end-to-end Quality of Service, tailored security and performance management afforded by such a device. SDMs provide predictable high-quality voice, video and time-sensitive data - including legacy serial data - over IP networks, delivering traffic as reliably as Time-Division Multiplexers.

There are many functions addressed by SDMs on the market today, each of which addresses specific customer requirements. To put the differing implementations into perspective, we offer the following taxonomy (*see Figure 1*[1]).

[1] Figure 1 is derived from "Pocket Guide to Application Delivery Systems", P. Sevcik and R. Wetzel, 2006.

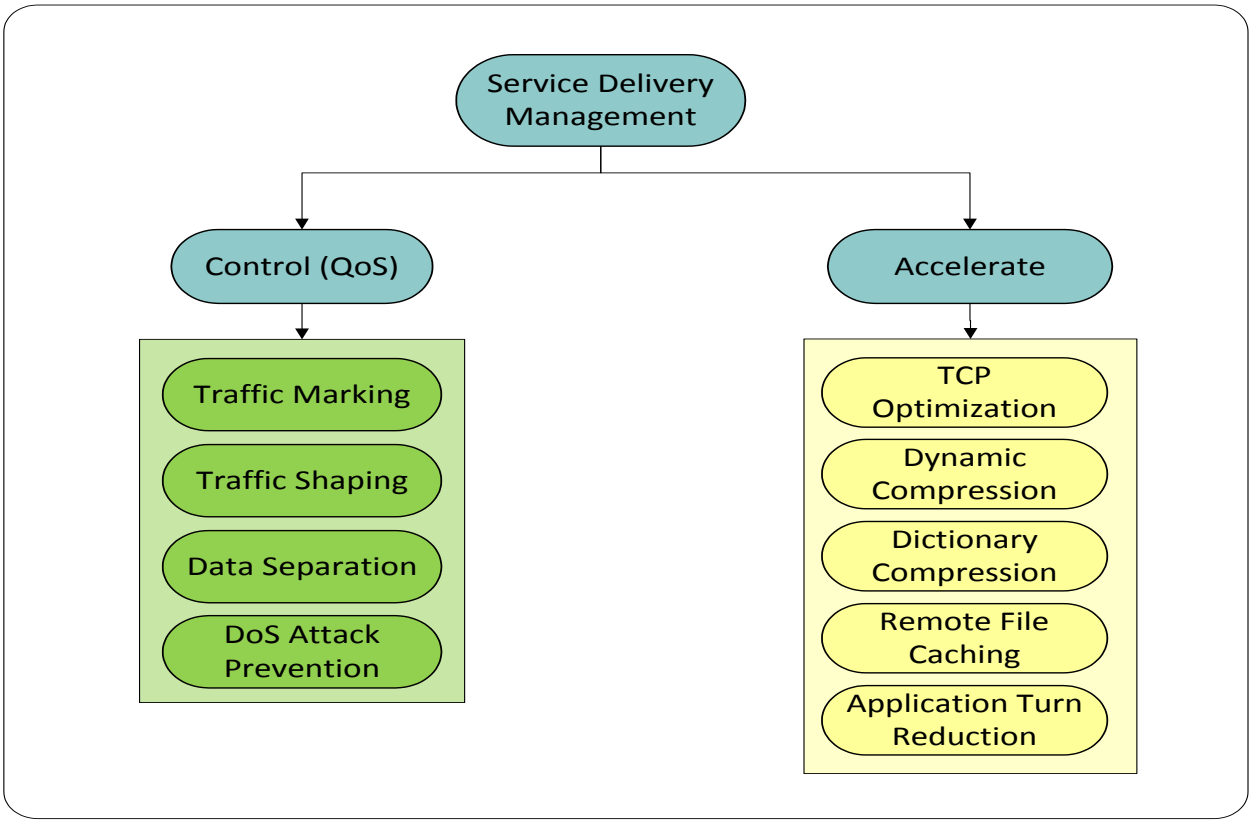

Figure 1: Service Delivery Management Taxonomy

In this taxonomy, Service Delivery Management is categorized into the following:

- Control – control solutions protect service delivery from degradation by applying traffic marking, shaping, data separation and denial-of-service attack prevention to help ensure Quality of Service (QoS).
- Acceleration – acceleration solutions speed up service delivery by reducing payloads or otherwise changing how a service behaves over a WAN link to make it faster.

While each solution has its own merits and seeks to solve the problems of service delivery in different ways, it is important to avoid using acceleration techniques without also deploying control solutions. Acceleration in the absence of control is not recommended because performance for accelerated services can still deteriorate badly under adverse network conditions. The ideal solution is to ensure that one has considered control and acceleration when designing a network.

Effective SDMs will perform several of the functions listed above in Figure 1 rather than forcing users to deploy appliances for each of the functions. As an example, an SDM could be designed to adapt, classify, shape, cross connect, policy enforce, mark, schedule and queue traffic in a single hardware platform . Network architects need to evaluate which functions can be combined to minimize the number of devices in the network without relying on

any single device to the point of a degradation in performance.

Allocating network resources to the various services required by the Department of Defense requires a standardized method to mark, or designate the relative priority of traffic flows. The DoD strategy is to use Differentiated Services Code Points (DSCPs) to mark traffic. While some applications and most routers are able to set DSCPs, SDMs offer the most flexible, simple and cost-effective solution for marking traffic, which is required for the anticipated transition of the DISN to Unified Communications.

Modern routers are often considered acceptable substitutes for dedicated SDMs, but in practice the additional burden placed on a router to perform sufficient QoS functions leads to performance degradation of the router. This usually results in expensive add-ons to the existing router, or even upgrading the entire router to a more capable (and expensive) model. Better to let the router do just the routing, and leave the QoS control and cross-connects to a specialized SDM platform that contains the high speed hardware switching and memory designed for the job.

Distributed SDMs are usually placed at the point of user access to converged services, where traffic preferences and priorities are evaluated in real time (*Figure 2*). This ensures that services are delivered to end users correctly, in the appropriate time frame, and in relative accordance with the priorities required by other competing services delivered to/from the WAN. Alternatively, SDMs can also be placed at lower layers of a network where multiple traffic flows converge and decisions regarding priorities and traffic marking need to be made.

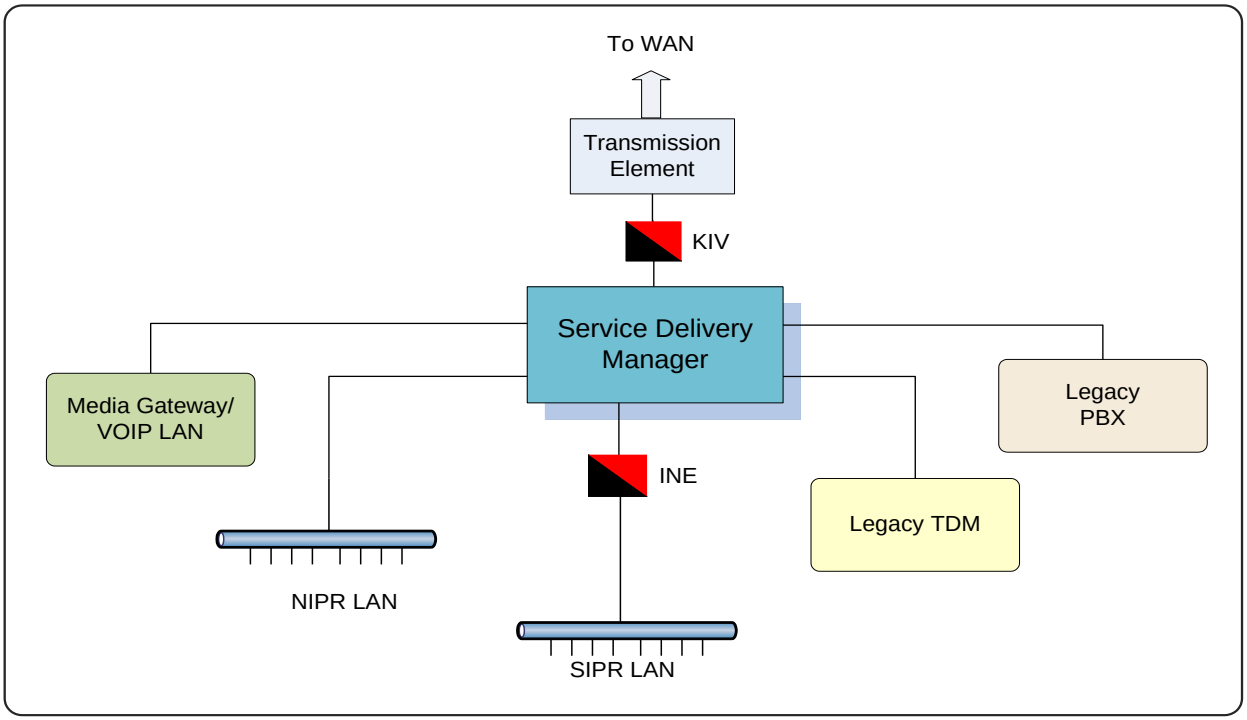

Figure 2: Service Delivery Manager at Point of Convergence

SDMs destined for tactical use must possess unique characteristics, in contrast to traditional offerings normally associated with commercial IT implementations. Tactical SDMs must first meet Department of Defense requirements for service classification and differentiation, including:

- Fine-grained Quality of Service
- Access to the Colorless Core
- Custom service classifications
- Interoperability with multiple, varied transmission technologies
- Comms-on-the-Move

Additionally, tactical SDMs must realistically address the incremental transformation of military networks by supporting legacy and IP domains, on both the user side and the WAN side, concurrently. This typically means that a mix of interfaces must be available, including Ethernet, EIA 530 Serial, T1/E1, and TADIL, at a minimum, to support the wide range of systems currently deployed. Information Assurance controls must be embedded to enable secure operation during any mission. Finally, the overall hardware architecture must be enhanced beyond the standard COTS design goals to ensure reliable operation in environmental and operational extremes.

About Ultra Electronics DNE Technologies

For over fifty years, Ultra Electronics DNE Technologies has provided communications devices to the US Department of Defense, Homeland Security and other government agencies. Ultra Electronics DNE Technologies manufactures networking equipment that economizes bandwidth and extends the drive distances of tactical communications devices. This equipment is used throughout the US Department of Defense and other government agencies to support the transition to IP networking, particularly in areas where bandwidth-intense network traffic is restricted by a single satellite or radio signal. Ultra Electronics DNE Technologies manufactures the AN/FCC-100, the TAC Multiservice Access Concentrator series, PacketAssure Service Delivery Managers and NRZ/CDI/FOM converters, including the CV-MCU2 converter/multiplexer.

50 Barnes Park North • Wallingford, CT 06492 • p 800.370.4485 • f 203.697.6592
www.ultra-dne.com • info@ultra-dne.com