DNE TECHNOLOGIES

White Paper

Implementing an IP Architecture Using Layer 2-Based Traffic Management

17 October 2009

Implementing an IP architecture involves a number of challenges. The foremost challenge is that in most instances a Greenfield implementation is not possible and legacy services or equipment will need to be supported. Another key factor is that while the commercial marketplace offers network models for the Department of Defense (DoD), there are significant differences among DoD architectures that need to be addressed, such as TRANSEC and MLPP. [1] [2] [3]

One of the advantages of IP traffic also presents a challenge. Although Ethernet and IP technologies are designed to avoid congestion, and these technologies can be forgiving when packets are lost or damaged, significant congestion can severely impact applications in unpredictable ways. A few packets of User Datagram Protocol (UDP) traffic, such as a voice call, can typically be lost without significantly impacting the quality of the user application. Transmission Control Protocol (TCP) traffic, such as email, that has been damaged or dropped will be retransmitted. The challenge is that when a convergence point reaches a congested state, a much greater number of packets may be impacted. This will not be tolerated by the delay sensitive UDP traffic and may impact some of the TCP traffic as well. Typically, the

[1] Christopher Mellon, "It's the architecture!" *Signal* August 2007.
[2] Stew Manuson, "Broadband on the Battlefield," *National Defense* January 2009.
[3] Robert Ackerman, "Commercial Technologies Manage Navy Networking," *Signal* May 2008, p.55-56

convergence device will restrict all traffic flows when it senses congestion on any one input stream, impacting all services and prolonging retransmission of dropped TCP packets from all of these services. The convergence device must be able to process all of the traffic, make decisions regarding which traffic is to be given priority, and make decisions as to what to do with traffic that is not high priority.

Network architects that only have routers as convergence devices are faced with the choice of using large buffers to hold the packets until the congestion subsides or in artificially constraining the input ports to avoid congestion altogether. The first choice causes increased latency and jitter in the network, which results in diminished performance of some applications such as real-time services. Artificially constraining the input ports diminishes the dynamic bandwidth allocation benefit of IP and moves the network back towards a TDM-based architecture. Network architects need to ensure that their convergence devices perform in a predictable and consistent manner when faced with congestion, without diminishing the benefits that IP and Unified Communications offer.

Network architects can also face a challenge in choosing the appropriate sized router for their network when routers are their only choice. Although routers perform various functions that include routing, traffic management, cross connections and protocol adaptation, these services are largely done in software; putting a demand on the memory and processors of the router. As the functions the router must support expand, so must the memory and processing capacity of that router. Network planners will be forced to either migrate to more expensive, higher-class routers or partition the services over multiple routers. Either option significantly increases the network costs.

The need for traffic management in IP networks is also impacted by the need for security within the DoD. In order to provide security for DoD traffic, encryption must be employed. Encryption can be another drain on processing power within a convergence router, but more importantly it can impact the router's ability to make traffic management decisions. Commercial practices are typically only concerned with encrypting the data within packets but the DoD also has security concerns about the broadcast of particular IP addresses, the type of packet that is being transmitted and any patterns that can be discerned from the traffic. Encrypting all of this information blocks the convergence device's ability to make traffic management decisions. Proposals to copy Differentiated Services Code Points (DSCPs) into the cipher text header alleviate this problem only if the originating devices have marked all of the traffic with DSCPs and the convergence device can make this decision without adding additional latency.

Another challenge facing the DoD is that the expansion of Beyond Line Of Sight (BLOS) bandwidth has not evolved as fast as had been projected. The cancellation of the TSAT program and delays in WGS have diminished the availability of government-owned satellite capacity, forcing the DoD to either increase the use of expensive commercial satellite bandwidth or to move forward with less bandwidth available. Either way, these circumstances may result in more instances of congestion, greater expense and more traffic management challenges.

A final challenge is that the connectionless nature of IP traffic raises the complexity level for operators of a network. While the connectionless nature allows for great amounts of architectural flexibility and efficiency, it also is more complex to manage than TDM traffic. When combined with the challenges listed above, it becomes imperative that network operators receive more training that has been necessary in the days of TDM. Current operators of IP-based systems are undergoing as much as 180 days of training prior to being qualified to operate these systems.

Specialized network processors found in Layer 2 devices can bring enormous computing power to bear on managing IP traffic at the link level. This computing resource can implement dozens of traffic management policies which can carry service preferences down to the user, a group of users, or an application while operating at line speeds in the gigabit per second range. This performance level is achieved by dedicating the processor to traffic management tasks only. As discussed above, a convergence router has to distribute its general processing power across various tasks, limiting performance as requirements increase. Hardware-based appliances offer an opportunity to offload some of this functionality, while keeping costs and network complexity in check.

The general wisdom in the commercial world is that the key to maintaining IP service quality is to provision enough link bandwidth so that links are never fully utilized. In the tactical military world where beyond-line-of-sight bandwidth is scarce and expensive, that strategy is not viable. Many military units continue to use time-division multiplexing technology to separate Real Time Services and critical data from the rest of the network, assuring that the time-sensitive services are adequately provisioned. A Layer 2-centric device understands the capacity of the congested link and can use traffic policies to delay transmission of lower-priority traffic. The Layer 2 approach will keep the transmission link filled during both congested and non-congested periods. An IP router or Layer 3 device discards traffic until the congestion period passes and the amount of data in the buffer starts to diminish. The Layer 3 approach will be far more disruptive, and limiting user access to the network to avoid congestion is not a preferred strategy. A consequence to the Layer 3 strategy of restricting bandwidth is that, even in non-congested periods, the full transmission link capacity will be limited since bandwidth must be reserved only for use by high priority traffic. This is not the case with a Layer 2 device that manages traffic by classifying flows and defining precedence on a per-flow basis.

A key requirement of tactical applications is that unified networks can adapt quickly to meet the mission as mission requirements change. A Layer 2 device can change traffic priorities quickly by directly modifying the detailed configuration or uploading a pre-defined configuration template without any risk to network stability. IP router operators avoid modifying traffic management parameters without first testing them offline. As IP router traffic management is a delicate balance of policies, CPU and memory resources, a miscalculation in modifying a configuration can crash the router. The stability of the Layer 2 device and its easily understood configuration rules allows for a network operator with a basic understanding of IP networking to operate

the device without extensive training certifications and specialization.

The flow-based nature of Layer 2 also offers advantages in troubleshooting. While Layer 3 provides great flexibility with routing, it can also be extremely difficult to troubleshoot. Mihai Puchio from IP test manufacturer IXIA claimed that IP network troubleshooting can take as much as four times the amount of time as TDM networks.[4] Using flow-oriented troubleshooting and Layer 2 technology minimizes this time by combining the clarity of connection-based network architectures with the dynamic bandwidth benefits of IP.

[4] Mihai Puchiu, "VoIP Quality Testing in a UC Environment" Ixia TV: Webinars, May 14, 2009

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.

This document has been released for general distribution.

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