Supporting Mission-Critical Applications over Multi-Service Networks

C. Christou[1], M. Davenport[2]

[1] Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA, USA 22102
christou_chris@bah.com
[2] Booz Allen Hamilton, 5220 Pacific Concourse Drive, Los Angeles, CA, USA 90045
davenport_michael@bah.com

Abstract. Future government IP networks must satisfy mission-critical QoS requirements that are introduced by high-priority customers. A prime example includes the Multi-level Precedence and Preemption (MLPP)-like requirements. This paper will focus on the challenges in satisfying these needs in future government IP networks.

1 Introduction

Government organizations, to save on long-term operational expenditures, have begun migrating services (i.e., voice, video, mission critical applications) to a single IP-based infrastructure. For example, the US Department of Defense (DoD) has outlined its intent to transition to IPv6 by 2008, facilitating its transformation to net-centric operations [1]. Therefore, the demand for converged services over IP networks to support critical operations introduces new challenges. Future networks will need to support a MLPP-like service which was offered over legacy circuit-based networks. In addition, future designs will have to provision these services over wireless networks, introducing challenges when trying to guarantee service. Finally, the architecture should be balanced with the security requirements that must be simultaneously satisfied.

2 QoS for Mission Critical Applications over Wireless Networks

The first step for developing QoS requirements for any network involves enumerating the types of applications that will be transported over the infrastructure and categorizing them into Service Classes. Although the Service Classes defined for the Internet in [2] apply to government users, some applications that are not necessarily unique to government users but are mission-critical to their communities could include telemetry, command and control, and high quality video/imagery. In these cases, special service classes might be required. However, the uniqueness of these applications is an area requiring further study.

Additional requirements related to QoS exist that are unique to the military and mission-critical networks. As discussed in [3], MLPP is a service currently offered in legacy circuit networks, providing commanders the ability to allow for the communication of high precedence calls during times of crisis. In general, MLPP offers the ability for high precedence calls (e.g., flash) to preempt lower precedence ones (e.g., routine) during times of congestion. Future IP networks will need to support this service not only for telephony, but for other inelastic and elastic services as well. Several architectures, including those mentioned in [3] and [4], have been proposed to satisfy both QoS and MLPP requirements. Most importantly, the use of QoS signaling protocols to provide service guarantees and admission control in support of inelastic services and MLPP is a strong consideration. Nevertheless, in trying to assess the applicability of these architectures to future systems, the performance characteristics of future networks must also be considered. Most importantly, military and humanitarian missions will increasingly rely on wireless networks, including satellite IP-based networks and Mobile Ad-hoc Networks (MANETs), for their communications needs. Therefore, QoS mechanisms must be applied carefully to these diverse infrastructures to ensure that MLPP-like services, and service quality in general, are provided.

With respect to satellite networking, the use of Demand Assigned Multiple Access (DAMA) techniques are increasing due primarily to the gains that can be achieved through bandwidth sharing for multiple connected regions. However, there are issues with this increased use due not only to their high Bit Error Rate (BER) but also the instability of the BER. For example, the provisioning of guaranteed services could result in a reduction in RF link utilization, which could be extremely costly considering the limitations of RF communications with respect to capacity. For MANET communications, the fact that they have dynamic topologies with limited security make the provisioning of signaling mechanisms/guaranteed service much more challenging due to routing instabilities and variable bandwidth. Therefore, further analysis is needed to determine whether a signaled approach is a viable solution for wireless networks while understanding whether the utilization for providing guarantees is too costly.

3 QoS and Levels of Assurance

In addition to supporting policy requirements (e.g., MLPP), future networks will also require high levels of information assurance (IA) with respect to authentication, integrity, and protection. Therefore, these separate IA, QoS, and policy requirements present a common tradeoff: one must provide functionality to end users while preserving a secure infrastructure. With IP networks implementing IP encryption and authentication closer to the network edge, providing high levels of QoS for end-to-end guarantees becomes increasingly difficult. As proposed in [3], one can leverage the Resource Reservation Protocol (RSVP) to offer MLPP services over IP networks . However, depending on the policy and security requirements, end-to-end RSVP signaling may not be permitted across all networks. Even in cases where QoS signaling is allowed, individual domains must implement

strong Authentication and Authorization mechanisms if accepting resource requests from external networks. In addition, the security risks associated with including information in data plane packet headers must be considered. Therefore, the QoS architecture that is applied across networks may differ depending on the security requirements—in some cases network engineers may have more flexibility in the functionality that is permitted. However, for more sensitive cases, the mechanisms that are applied may be more limited due to more heightened security risks.

4 Conclusion

In this paper we addressed the trend towards migrating all services to a single IP-based infrastructure. Examples of this trend include the US DoD's current transition to an IPv6-based infrastructure. The challenges outlined in this paper include: supporting IP QoS over multiple environments and the integration of IA and QoS. In particular for government IP networks, they must not only satisfy end user performance requirements but also provide MLPP-type services for high priority users. However, providing QoS with MLPP becomes difficult due to the types of networks that will be deployed. For example, the approach to addressing the issues in wireless environments must take into account the dynamic nature of mobile and satellite IP networks. In addition, regardless of the network over which converged services will be deployed, strict IA requirements must be taken into consideration. As these next generation networks mature, organizations such as the Internet Engineering Task Force must continue to develop additional standards, new approaches, and new analysis techniques to provide an architecture which balances these special needs and maximizes utilization for all environments.

References

1. Kraus, Marilyn (2003) *DoD Transition to IPv6*. In: US IPv6 Summit 2003, 8-11 Dec 2003, Washington D.C. http://www.6journal.org/archive/00000057/01/Marilyn_Kraus.pdf
2. J. Babiarz, K. Chan, F. Baker (2004) *Configuration Guidelines for DiffServ Service Classes*. draft-baker-diffserv-basic-classes-04. http://www.ietf.org/internet-drafts/draft-baker-diffserv-basic-classes-04.txt
3. F. Baker and J. Polk (2005) *Implementing MLPP for Voice and Video in the Internet Protocol Suite*. draft-ietf-tsvwg-mlpp-that-works-00. http://www.ietf.org/internet-drafts/draft-ietf-tsvwg-mlpp-that-works-00.txt
4. M. Pierce and S. Silverman (2005) *Multi-Level Expedited Forwarding Per Hop Behavior (MLEF PHB).* draft-silverman-tsvwg-mlefphb-02.txt. http://www.ietf.org/internet-drafts/draft-silverman-tsvwg-mlefphb-02.txt.