Paper

A concept of Differentiated Services architecture supporting military oriented Quality of Service

Marek Kwiatkowski

Abstract — This paper presents a concept of IP Differentiated Services (DiffServ) architecture in conjunction with bandwidth brokerage and policy based network management, all aimed at efficient and flexible provision of the military oriented Quality of Service (M-QoS) features in the Australian Defence (strategic) wide area network and its satellite trunk interconnections with the tactical domain. Typical DiffServ functions are analysed in the paper with regard to their roles in offering M-QoS. Some preliminary simulation results of applying these mechanisms to achieve traffic policing and differentiation for (UDP) video traffic streams, are also presented. Finally, the paper proposes the use of bandwidth brokerage in each DiffServ domain to facilitate automatic Service Level Specification (SLS) arrangements with end-user applications, and policy based network management to support the flexible implementation of bandwidth brokerage.

Keywords — Quality of Service, military networks, Differentiated Services, bandwidth brokerage, policy based network management.

1. Introduction

The term military oriented Quality of Service, introduced in [1], represents commercial QoS in conjunction with the following features. Firstly, in military packet networks, when not enough network resources are available to support QoS for all traffic flows, the flows carrying mission critical information should get preference (i.e., higher priority) over less important flows. Secondly, in overloaded networks, it is preferable to gracefully "step down" the hard QoS[1] of less important military flows instead of automatically tearing down these flows. Finally, higher flow priorities should be given for a restricted time defined by an enterprise policy.

IP differentiated services is a promising new technology that could facilitate implementation of M-QoS in the Australian Defence strategic and tactical packet communication environment [2]. This is mainly because this technology is scalable, can provide both hard[2] and soft QoS as well as graceful degradation in hard QoS to IP flows. However, DiffServ does not specify a standardised user network interface to negotiate service level specification in an automated fashion.

This paper presents a novel concept of IP DiffServ architecture in conjunction with bandwidth brokerage and policy based network management[3], all aimed at efficient and flexible provision of the M-QoS features in an IP-oriented subset of the long-distance Australian Defence Core communication environment (further called Defence Core for short). This subset is composed of: (1) packet oriented strategic (terrestrial) networking infrastructure composed of the IP-based routing backbone network and the ATM-based Defence Corporate Backbone Network (DCBN); and (2) Geo-synchronous Earth Orbit (GEO) satellite infrastructure used to: (a) interconnect the strategic network with tactical trunk networks; and (b) provide back-up connectivity for the strategic network.

It is stressed that currently the considered environment only offers best effort service. On the other hand, it is expected that the same environment will soon carry bulk defence multimedia (i.e., voice, video and data) traffic of different importance. It is vital to provide the M-QoS features not only in bandwidth-impoverished parts of the Defence Core (such as satellite links), but also as broadly as possible. The reason for the latter is the need to maintain the ability to transmit mission critical information even if the environment is partially destroyed.

The paper is structured as follows. Section 2 presents a general concept of the proposed architecture. DiffServ functions, bandwidth brokerage and policy based network management supporting bandwidth brokerage are described in more detail in Sections 3, 4 and 5, respectively. Conclusions and future work are given in Section 6.

2. General concept

Following the analysis provided in [2], Fig. 1 presents a combination of transmission technologies proposed to support M-QoS in the Defence Core. IPv4/IPv6 will generally be used for end-to-end communication across the (terrestrial/satellite) Defence Core between end-user applications to transfer multimedia information. An open question is whether Voice over IP (VoIP) can be carried over relatively slow satellite links. Note that DSTO is currently investigating this problem.

DiffServ will provide both hard and soft QoS as well as graceful degradation in hard QoS to IP flows. Both the strategic and tactical trunk networks will be divided into

[1] *Hard QoS* offers an absolute reservation of resources for specific traffic, while *soft QoS* provides to some traffic a statistical preference over other traffic.

[2] DiffServ can offer hard QoS through the use of an appropriate flow admission control and queueing mechanisms in routers.

[3] The term management refers here to longer time frame (e.g., hours, days) operations.

DiffServ domains. DiffServ will be augmented by the use of bandwidth brokerage. The latter will mainly be responsible for communication with end-user applications and flow admission control.

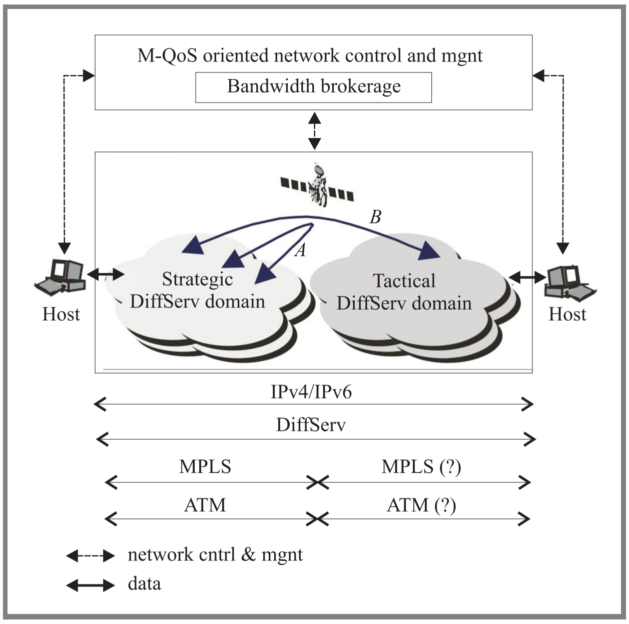


Fig. 1. General concept.

MPLS will be used to provide traffic engineering, mainly in the terrestrial part of the Defence Core. It seems to be desirable to use MPLS over a satellite to provide backup links to the terrestrial Defence Core (see *A* in Fig. 1), thus increasing its survivability. The use of MPLS between the strategic and tactical trunk domains (see *B* in Fig. 1) requires further study.

ATM will still be used in DCBN, firstly to support MPLS switching, and secondly to continue carrying voice traffic until VoIP is implemented on a large scale. ATM may be required to transport voice over slow satellite links if IPv4/IPv6 and DiffServ do not satisfy the low jitter requirements.

Figure 2 presents the proposed DiffServ architecture in more detail. The Defence Core routing environment will be divided into a number of DiffServ domains. Routers in each domain implement a number of Per-Hop behaviours (PHBs), each characterising the externally observable forwarding treatment applied at a DiffServ-compliant router to a collection of packets each having a distinct DiffServ Code Point (DSCP) value [3]. A maximum number of 64 PHBs can be created this way. Although, the parameters such as the number of PHBs, their characteristics and groupings will be decided in a relatively static fashion through an enterprise policy, we strongly suggest that packets representing different traffic types (e.g., file transfer, interactive, voice, video) and different military precedence levels (e.g., routine, flash) should belong to separate PHBs. This approach should facilitate dimensioning of network resources (e.g., buffers in routers) and flow admission control.

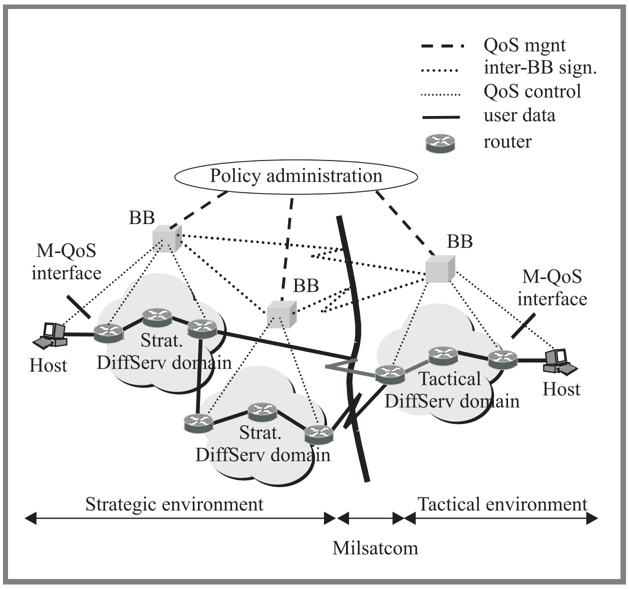


Fig. 2. Proposed concept of DiffServ architecture.

Each domain will be equipped with a single bandwidth broker (BB) entity. It will be responsible for automatic admitting to particular PHBs flows requiring (soft/hard) QoS and traversing the domain. To achieve this goal, the BB will communicate with:

- Local end-user applications (or their proxies) via a standard interface – to obtain information about parameters specifying the flows.
- Other BBs – to coordinate admission of flows that need to traverse a number of domains.

Note that BBs will not be involved in admitting best effort flows. In order to implement BB functions in a flexible and coordinated way amongst a number of BBs, policy administration will impose a single policy or a set of coherent policies onto BBs. It is assumed that these policies can often change, thus reflecting the dynamics of the battle space.

The next sections will present in more detail DiffServ functions, bandwidth brokerage and supporting it policy framework.

3. Differentiated services functions

To implement a PHB, Defence Core routers will use typical DiffServ functions such as packet classification, marking, metering, policing (dropping), shaping and queueing [3]. Below, we present how these functions can support M-QoS features in a generic way. Since primarily Cisco routers are used in the considered Defence Core environment, we will also discuss how these functions can be implemented using Cisco routers. It is noted that DSTO is currently conducting experiments with various configuration arrangements of DiffServ functions in Cisco routers.

3.1. Packet classification

Packets entering a router will be classified to one of the specified PHBs using filters. Our concept assumes that packets sent from end-user applications to ingress routers (IRs) will be classified based on the 5-tuple (source IP address, source port number, destination IP address, destination port number, and the transport protocol). The rules for classifying a flow in IRs will be delivered by the domain's bandwidth broker after deciding to admit the flow. All other (transit/egress/boundary) routers will have statically configured filters, which will classify packets based on their DSCP value set during packet marking (see below) in IRs.

We propose the use of Access Lists [4] to implement packet classification in Cisco routers.

3.2. Packet metering

Packet metering is used to measure temporal properties of a flow (flow aggregates) selected by the classifier against a traffic profile specified in a service level specification and/or against any relevant policy requirements. In our concept, packet metering will be required when implementing policing, shaping and queueing functions. As for Cisco routers, packet metering is in-built in the latter functions.

3.3. Packet marking

Packet marking is the process of setting the DSCP value in a packet based on defined rules. In our approach, packets are marked by IRs based on results of packet classification and metering. The rules for marking are specified by BBs at the time of admitting flows.

As for Cisco routers, marking will be implemented as a part of the policing mechanism (see below).

3.4. Packet policing

This process aims at discarding packets based on information provided by meters, and according to the rules specified by BBs.

In our concept, policing in IRs will be applied to all (military-essential) flows admitted by BBs. BBs will be responsible for sending to the routers a specification of dropping rules. This policing will be crucial to assure conformance of end-user application traffic to the previously negotiated SLS. It is stressed that individual best-effort flows will not be policed.

We propose the use of Two Rate Three Color Marker [5] to carry out packet dropping. In Cisco routers it can be implemented by Two-Rate Policer, which, as indicated above, also covers packet metering and packet marking.

3.5. Packet shaping

Packet shaping is a process of delaying packets within a packet stream to conform to some defined traffic profile. We expect that this function will be performed mainly by border routers to shape whole PHBs. Cisco routers offer Generic Traffic Shaping (GTS) [4] to do the shaping.

3.6. Packet queueing

From the perspective of our architecture, the following packet queueing features are desirable:

- Use of up to 64 queues representing different PHBs.
- Group PHBs into PHB Groups, each having a separate output queue.
- Differentiate between PHBs using the same queue.
- Allocate a minimum guaranteed bandwidth per each PHB Group, thus preventing bandwidth starvation of any PHB Group.
- Automatically re-allocate unused bandwidth to other PHBs that need it, thus providing efficient use of bandwidth.
- Offer absolute priority to some chosen PHBs – a feature crucial to implement real-time, low jitter traffic (e.g., voice).

With regard to Cisco routers, the following queueing mechanisms [4] can potentially fulfil the above features:

1. Class Based Weighted Fair Queueing (CBWFQ). This scheduling discipline enables the definition of up to 64 PHBs. PHBs can be grouped into classes (i.e., PHB Groups), each having assigned a minimum guaranteed bandwidth during congestion, weight and maximum length. The weight of a packet belonging to a specific class is derived from the minimum bandwidth assigned to the class. If a queue reaches its configured queue limit, enqueueing of additional packets to the class causes tail drop.
2. Weighted Random Early Detection (WRED). This mechanism is a combination of random early detection (RED) and DSCP-based precedence. Typical for RED lower/upper thresholds and the dropping probability for the upper threshold can separately be set for different DSCPs.
3. Low Latency Queueing (LLQ). When used with CBWFQ, LLQ allows delay-sensitive packets (e.g., carrying voice) to be sent first before packets in other queues, thus giving delay-sensitive traffic preferential treatment over other traffic. A single strict priority queue is maintained for the LLQ traffic.

We are currently considering an approach where PHBs representing the same traffic type are allocated to the same queues, and WRED is used to reflect military precedence mentioned in Section 2. CBWFQ will be used to differentiate between different traffic types (e.g., data bulk transfer, video, formal messaging).

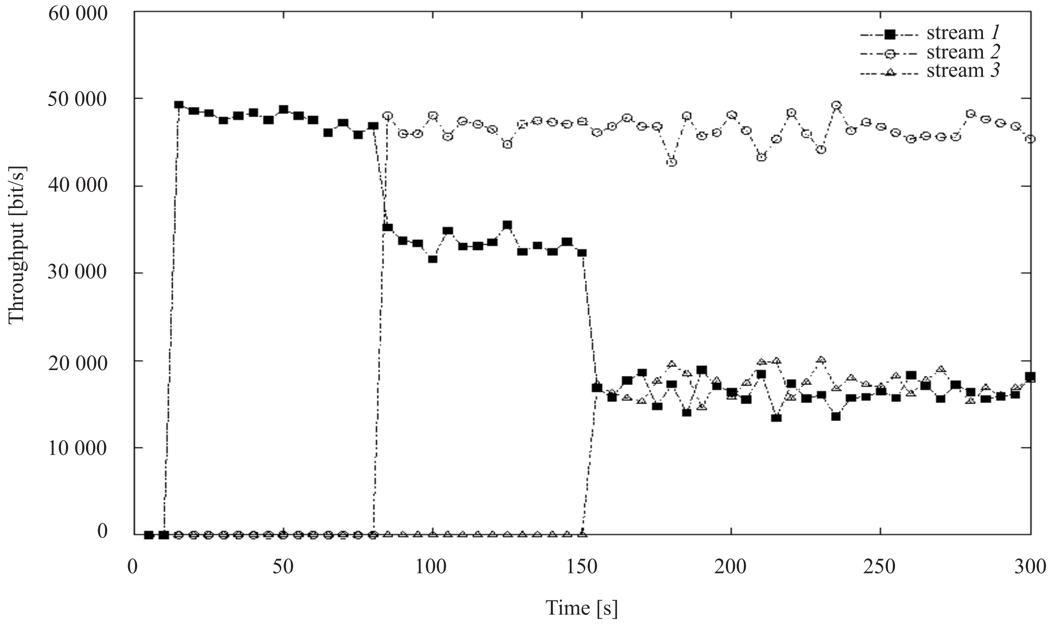


Fig. 3. Throughput versus time for (UDP) NetMeeting streams.

We have already done some preliminary simulation studies, using OPNET [6], to validate the above approach. Figure 3 shows throughput in five-second intervals obtained for three (UDP) NetMeeting [7] streams competing for the bandwidth of a 100 kbit/s link. Each stream, representing a "talking head", was first recorded on a real network and then sent in the simulation environment to a two-rate policer whose both peak rate and committed rate token buckets were set to the token replenishment rate equal to 50 kbit/s and the maximum burst size equal to 2000 bytes.

The non-conforming packets were lost. The policers also classified (using the DSCP byte) the conforming packets of streams *1* and *3* to a low priority, and of stream *2* to a high priority. Then, all the conforming packets were sent to a module simulating the WRED mechanism with two priority levels corresponding to the ones set by policers. The lower and upper thresholds for these levels were set to (1, 5) and (6, 10) packets, respectively. The thresholds were chosen to impose minimal queuing delay, and, at the same time, to enable traffic differentiation. For both priority levels, the packet dropping probability at the upper threshold was set to 0.1 and exponential weighting constant set to 2. The streams were initiated at approximately 1 min intervals to analyse the transients. It is visible in Fig. 3 that WRED gives consistent preference to the high priority stream, with no packets being dropped by WRED during the simulation run. The same figure also shows that WRED fairly divides the available bandwidth between the two low priority streams. This is confirmed by the average throughputs for streams *1* and *3* between times 170 s and 300 s being 16 234 bit/s and 17 439 bit/s, respectively. Note however, that as for TCP streams (e.g., see [8, 9]), WRED increases variability of the considered UDP traffic as well. For example, the coefficient of variation (i.e., standard deviation divided by mean) for stream *1* increases from 0.31 to 0.5, for stream *2* – from 0.31 to 0.54, and for stream *3* – from 0.32 to 0.49. More simulation/trial studies are planned for UDP and TCP streams to fully validate the presented approach.

Finally, note that a different approach to traffic differentiation, solely based on CBWFQ (i.e, with no WRED being used) is also being considered.

4. Bandwidth brokerage

We argue that the standard M-QoS interface described in [10] can be used to provide communication between an end-user application and its local BB. In brief, this interface enables the end-user application to specify for an IP flow a set of Commercial QoS Specific Parameters (e.g., peak rate, error rate, jitter) and a set of Military Specific Parameters (i.e., mission identification, precedence capturing both importance and timeliness, as well as user perceived priority). The same interface can also be used to inform the end-user application about any problems in delivering the requested/promised QoS. Finally, the M-QoS interface can be used by the end-user application to provide all the information required to perform authentication functions. Note that DSTO is currently building a prototype of an IP-based M-QoS interface using Java and Corba.

Our approach assumes that the commercial QoS parameters and military specific parameters are used by BBs involved in the admission process of the flow to evaluate the flow's ultimate priority, which corresponds to a particular PHB. Based on this evaluation, BBs decide whether to admit the flow to the PHB or not.

The ultimate priority evaluation is based on an algorithm defined by the policy implemented in the domain. Once the flow is admitted by all the involved BBs (and possibly by the receiving end-user application), the source BB orders the source IR to invoke appropriate classification, marking and policing functions (cf. Section 3).

It is stressed that in our approach, admission of a flow may result in degradation of other, less important flows, thus reflecting the idea of graceful degradation of QoS. This may also apply to hard QoS flows. For example, a flow carrying voice with precedence level flash can partially or completely preempt another voice flow having precedence level routine.

Other expected BB functions include:

- Evaluation of time restrictions related to the military precedence level of a flow. Such restrictions may trigger a change in the flow's classification (e.g., from flash to routine) at the flow's IR.
- Modification (if required) of reservations for pending flows.
- Organising monitoring of domain's resources and tracking SLSs of active flows.

Some form of inter BB communication is necessary to perform the above functions for cross-domain flows (cf. Fig. 2). We propose to base this communication on the Simple Interdomain Bandwidth Broker Signalling (SIBBS) protocol being finalised within the QBone Project [11, 12]. Note that DSTO is currently investigating the ability of this protocol to fully support the M-QoS requirements.

5. Policy framework

The proposed approach to policy-based M-QoS management uses the IETF policy framework [13], and comprises the following generic components:

a. Policy administration (PA) – responsible for consistent DiffServ offerings across all Defence Core domains. It controls multiple BBs, automatically distributes changes to the policy, and correlates feedback from BBs regarding the health of their domains. Policy administration retrieves policies from a policy repository(ies).

b. Bandwidth broker/Policy Decision Point (BB/PDP) – plays a dual role, firstly acting as a PDP in relation to policy administration, and secondly performing typical bandwidth broker functionality.

c. Other policy servers – examples of such servers include an authentication server(s) and an accounting server(s).

d. Policy Enforcement Points – these are mainly DiffServ-enabled routers capable of enforcing QoS policy rules.

As depicted in Fig. 2, policy administration needs to cover both strategic and tactical DiffServ domains to provide end-to-end M-QoS. A complete centralisation of this administration in the strategic environment may not be desirable since a substantial amount of policy information may refer to these BB functions, which are strictly related to tactical domains operating in isolation. In such a case, sending to these domains all the policy details from a single strategic repository via relatively low bandwidth and unreliable satellite links may create performance and reliability issues. Therefore, it seems to be beneficial to distribute policy management. There are a number of possible approaches to such distribution. A plausible one is presented in Fig. 4, where a single strategic policy administrator (S-PA) controls all fixed DiffServ domains using a policy stored on its strategic policy repository (S-PR). In addition, each tactical DiffServ domain has its own PA (depicted as T-PA in Fig. 4) responsible for M-QoS delivery within the domain according to a policy stored on the tactical policy repository (T-PR). To achieve consistent M-QoS across strategic/tactical domains, all policies have to be coordinated using communication between S-PA and T-PAs across satellite links (Fig. 4).

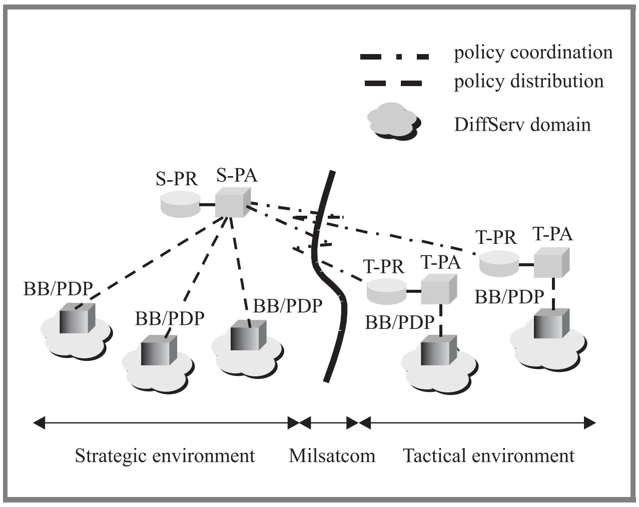


Fig. 4. Considered approach to policy distribution/coordination supporting bandwidth brokerage.

6. Conclusions and further work

In this paper we have proposed a flexible and scalable solution to implement M-QoS within the Australian Defence terrestrial/satellite Defence Core using differentiated services in conjunction with bandwidth brokerage and supporting it policy-based network management. Some encouraging preliminary simulation results of applying DiffServ mechanisms to achieve traffic policing and differentiation for (UDP) video traffic streams have been presented.

More simulation/trial studies are planned for UDP and TCP streams to fully validate the two approaches (i.e., with and without WRED) proposed in the paper. In addition, a number of other issues require further investigation, including:

- Design of viable flow admission control algorithm(s) and performance monitoring.
- Performance aspects (e.g., consumed bandwidth) related to inter-domain brokerage signalling over slow satellite trunks.
- Efficient and reliable distribution of policy administration for dispersed strategic/tactical trunk communications involving satellite communication.

Note that DSTO is currently investigating the first two groups of issues. It is also noted that DSTO is conducting research under the aegis of The Technical Cooperation Program (TTCP) [14] on the applicability of the proposed DiffServ architecture to a coalition environment.

Acknowledgments

The author would like to thank Mathew Elliot for providing the simulation results.

References

[1] M. Kwiatkowski and P. George, "A network control and management framework supporting military Quality of Service", in *Proc. IEEE MILCOM'99*, Atlantic City, USA, 1999, vol. 2, pp. 1161–1165.

[2] M. Kwiatkowski, "A Concept of Defence Core Communication Infrastructure Supporting M-QoS", (unclassified) DSTO Techn. Rep., DSTO-TR-1220, Oct. 2001.

[3] S. Blake *et al.*, "An Architecture for Differentiated Services", IETF, RFC 2475, Dec. 1998.

[4] Cisco IOS Release 12.2, 2001.

[5] Heinanen *et al.*, "A Two Rate Three Color Marker", IETF, RFC 2968, Sept. 98.

[6] OPNET, Version 8.0, OPNET Technologies Inc., 2001.

[7] NetMeeting, Version 3.01 for Windows, Microsoft Corporation, 1999.

[8] Th. Bonald, M. May, and J. Bolot, "Analytic evaluation of RED performance", in *Proc. IEEE INFOCOM'00*, 2000, vol. 3, pp. 1415–1424.

[9] S. H. Low *et al.*, "Dynamics of TCP/RED and a scalable control", in *Proc. IEEE INFOCOM'02*, New York, USA, 2002, vol. 1, pp. 239–248.

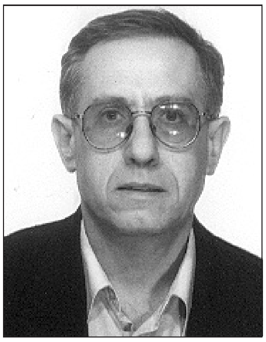
[10] P. Blackmore, P. George, and M. Kwiatkowski, "A Quality of Service interface for military applications", in *Proc. IEEE MILCOM'00*, Los Angeles, USA, 2000, vol. 1, pp. 470–474.

[11] B. Teitelbaum *et al.*, "Internet2 QBone: building a testbed for differentiated services", *IEEE Network*, vol. 13, no. 5, pp. 8–16, 1999.

[12] QBone Signaling Design Team,
http://qbone.internet2.edu/bb/index.shtml

[13] IETF, Policy Charter,
http://www.ietf.org/html.charters/policy-charter.html

[14] The Technical Cooperation Program (TTCP),
http://www.dtic.mil/ttcp



Marek Kwiatkowski received the M.Sc. degree from the Silesian Technical University, Gliwice, Poland in 1979 (computer science), and the Ph.D. degree from AGH University of Technology, Cracow, Poland, in 1990 (telecommunications). From 1991 until 1998, he worked at the Teletraffic Research Centre, University of Adelaide, Australia, first as a Post Doctoral Fellow, and from 1995 as a Research Fellow. Since June 1998 he has been working at the Communications Division of the Defence Science and Technology Organisation (DSTO), Adelaide, as a Senior Research Scientist. His main research interests include control and management aspects of narrowband and broadband networks.

e-mail: marek.kwiatkowski@dsto.defence.gov.au
Defence Science and Technology Organisation
PO Box 1500, Edinburgh, SA 5108, Australia