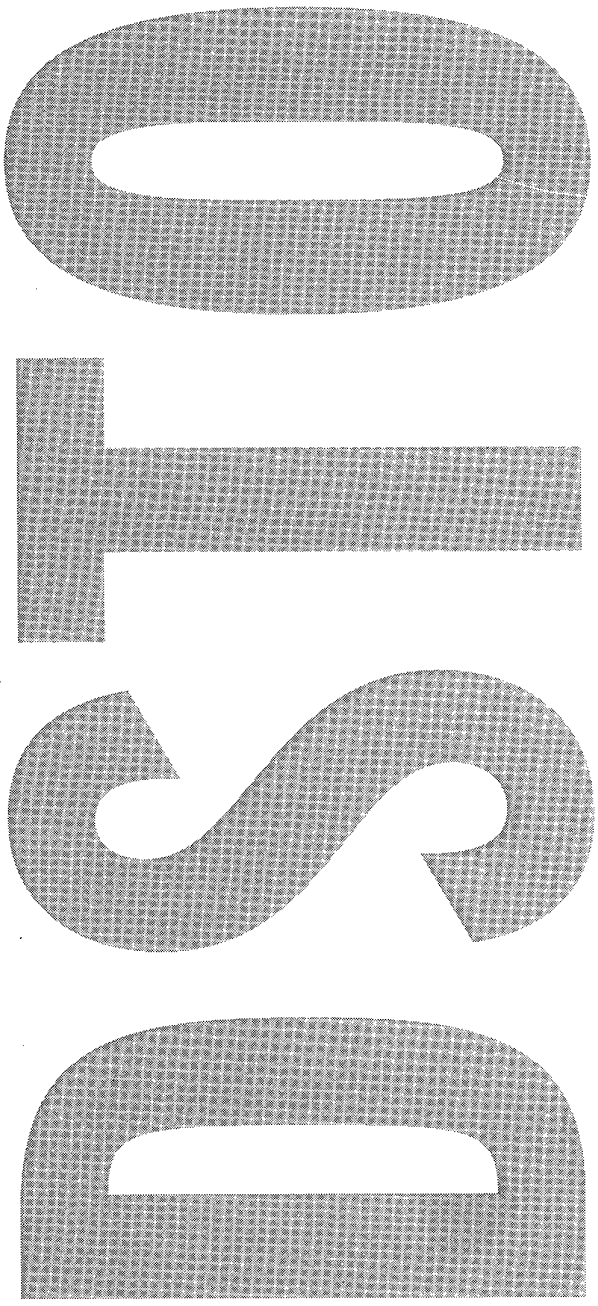
DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO



Preliminary Assessment of Transmission technologies to Support Military Oriented QoS

Marek Kwiatkowski

DSTO-TR-1207

Preliminary Assessment of Transmission Technologies to Support Military Oriented QoS

Marek Kwiatkowski

Communications Division
Electronics and Surveillance Research Laboratory

DSTO-TR-1207

ABSTRACT

This report is aimed at assessing some promising available or emerging commercial transmission technologies regarding their potential support of Military oriented Quality of Service (M-QoS) in the terrestrial/satellite Defence Core communications infrastructure. The chosen technologies are ATM, IP Integrated Services, IP Differentiated Services, MPLS and IPv6. The criteria of interest include the support of commercial QoS, prioritisation/preemption, graceful degradation of QoS, QoS interface with end-user applications, QoS modification, traffic engineering, scalability, bandwidth usage efficiency, and implementation in commercial as well as military networks. The report shows that none of the considered technologies can support all the criteria in isolation. However, a combination of IPv4/IPv6, Differentiated Services (augmented by bandwidth brokerage), MPLS and in some cases ATM is proposed in the report as a good candidate to build the future M-QoS capable Defence Core. More research is required to fully assess the applicability of the proposed combination to achieve M-QoS.

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-012-014
September 2001

Preliminary Assessment of Transmission Technologies to Support Military Oriented QoS

Executive Summary

This report is aimed at assessing some promising available or emerging commercial transmission technologies regarding their potential support of Military oriented Quality of Service (M-QoS) in the terrestrial/satellite Defence Core communications environment.

Delivering Quality of Service (QoS) to support mission-critical and time sensitive traffic has become a significant technical challenge for commercial service providers using packet Wide Area Networks (WANs). This refers to both hard QoS (i.e., when the network offers an absolute reservation of resources for specific traffic) and soft QoS (i.e., when some traffic is offered a statistical preference).

In military packet networks, when not enough network resources are available to support hard QoS for all traffic flows, the flows carrying mission critical information should get preference (i.e., higher priority) over less important flows. In addition, in overloaded networks, it is preferable to gracefully "step down" the hard QoS of less important military flows instead of automatically tearing down these flows. Commercial QoS in conjunction with flow prioritisation (according to the military value) and graceful degradation in hard QoS is jointly called Military oriented QoS (M-QoS). Today's packet based ADF networks do not support M-QoS.

The basic components involved in delivering the M-QoS include: (a) a standardised M-QoS interface between a military end-user application and the network management and control; (b) transmission infrastructure, which supports (commercial) QoS features; and (c) military oriented network control management.

This report is a continuation of the DSTO's research effort to propose technical solutions enabling M-QoS features in the Defence terrestrial/satellite Core communications infrastructure. The previous research has mainly been related to the design of a standardised M-QoS interface, while this report is focussed on the transmission infrastructure aspects (see (b) above) in relation to the provision of M-QoS.

In particular, the report aims at: (A) undertaking a preliminary assessment of promising commercial transmission technologies in their potential support of M-QoS for a chosen subset of the Defence Core; and (B) proposing the best candidate(s) among these technologies for a more thorough analysis. The subset of the long-distance Defence Core communications environment chosen for the analysis is composed of: (1) Packet oriented fixed (terrestrial) networking infrastructure (called fixed network for short), used for strategic communications and composed of the Backbone Routing Service (BRS), the Secure Backbone Routing Service (SECBRS) and the Defence

Corporate Backbone Network (DCBN); and (2) Packet oriented satellite infrastructure used to: (a) interconnect the fixed network with the (mobile) tactical infrastructure using trunks (called in this report tactical trunk network); and (b) provide back-up connectivity for the fixed network.

The report is focused on using this environment for Local Area Networks (LANs)/Base Area Networks (BANs) connectivity. It is noted that the chosen environment is becoming crucial in carrying bulk Defence multimedia traffic. Within this environment, only the ATM-based DCBN offers hard/soft QoS. The IP-oriented BRS and SECBRS networks only offer the best effort service.

The transmission technologies chosen for assessment include ATM, IP Integrated Services, IP Differentiated Services (DiffServ), Multi Protocol Label Switching (MPLS) and IPv6. These technologies are either already implemented or can potentially be implemented in the Defence Core.

The criteria for assessment include the support of the commercial QoS, prioritisation/preemption, graceful degradation of QoS, QoS-aware interfacing between a network and end-user applications, QoS modification, traffic engineering, scalability, bandwidth usage efficiency, and implementation in commercial as well as military networks.

The report refers to short to medium term (2-5 years) design goals.

The most important findings of this report are as follows:

a. None of the analysed transmission technologies supporting commercial QoS can completely fulfil the criteria considered in this report as vital to implement M-QoS in the Defence terrestrial/satellite Core;

b. The report proposes to use IPv4/IPv6, DiffServ, MPLS and ATM as building blocks for the future M-QoS capable Defence Core. Both fixed and tactical trunks Defence networks will be divided into DiffServ domains, each equipped with a bandwidth broker responsible for the proper provision of bandwidth within its domain, and between its domain and peer domains;

c. In the proposed transmission framework, Bandwidth Brokers (BBs) are the only entities performing military specific functions. All other entities are typical commercial solutions;

d. The report identifies Policy-based Network Management (PBNM) as an important mechanism to facilitate the implementation of M-QoS in a flexible way;

e. For the proposed combination of technologies, a number of issues require further study, among which the most challenging are:

   - Bandwidth implications for BB-to-BB communication over a satellite link;
   - Relationship between Bandwidth Brokers and PBNM in the Defence context, and performance implications of using PBNM to manage strategic and tactical DiffServ domains connected by a satellite link;
   - Impact of the proposed combination of technologies on the currently used/planned security architecture(s) for the Defence Core.

Based on the report's findings, the following is recommended:

A. Prepare a concept of network transmission, control and management architecture that would offer M-QoS features over the Defence terrestrial/satellite Core environment communications infrastructure;

B. Undertake a detailed study on how PBNM could be implemented in an efficient and reliable way in the Defence terrestrial/satellite Core environment;

C. Analyse the impact of the Defence Core security architecture on the proposed transmission infrastructure.

Authors

Dr Marek Kwiatkowski
Communications Division

Dr 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, Cracow, Poland, in 1990 (Telecommunications). From 1991 until 1998, he worked at the Teletraffic Research Centre, University of Adelaide, first as a Post Doctoral Fellow, and from 1995 as a Research Fellow. Since June 1998 he has been working at the DSTO, Network Integration Group, as a Senior Research Scientist. His main research interests include control and management aspects of multimedia military and commercial networks.

Contents

1. Introduction

This report is aimed at assessing some promising available or emerging commercial transmission technologies regarding their potential support of Military oriented Quality of Service (M-QoS) in the terrestrial/satellite Defence Core communications environment.

Delivering Quality of Service (QoS) to support mission-critical and time sensitive traffic has become a significant technical challenge for commercial service providers using packet Wide Area Networks (WANs).

Following the ITU rec. M60 [M60], Quality of Service (QoS) is understood in this report as the collective effect of service performances, which determine the degree of satisfaction of a user of the service. Performance measures include amount of bandwidth, transmission delay, jitter and error rate. Note that QoS is an end-to-end issue that relates to all networks involved in transmitting user information.

Generally, two basic types of QoS can be provided [QOSF99]:

- *Hard QoS* – the network offers an absolute reservation of resources for specific traffic; hard QoS is particularly important when a real-time flow[1] is to be transmitted, such as streamed video or audio;
- *Soft QoS* – some traffic is offered a statistical preference (e.g., faster packet handling, lower probability of packet discards) over the rest.

In this report, the term "QoS" alone will mean both types of QoS.

Currently, a number of already available and standardised packet-oriented commercial transmission technologies, such as ATM and IP Integrated Services (IntServ), can provide QoS. However, a set of new, sometimes not fully standardised technologies supporting QoS are emerging, including IP Differentiated Services (DiffServ) and Multi-protocol Label Switching (MPLS).

In commercial networks, if not enough free network resources are available to establish/maintain a flow with the required hard QoS, a typical approach is to release the flow, and offer no graceful degradation in QoS.

However, as argued in [KWIA99a], in military packet networks, when not enough network resources are available to support hard QoS for all traffic flows, the flows carrying mission critical information should get preference (i.e., higher priority) over less important flows. In addition, in overloaded networks, it is preferable to gracefully "step down" the hard QoS of less important military flows instead of automatically tearing down these flows. The end-user application, rather than the network, should decide whether the offered hard QoS is sufficient to continue the flow. On the other hand, the network, not the end-user application, decides whether and which flows

[1] Following [SHEN97], a flow is understood in this report as a set of packets traversing a network, all of which are covered by the same request for control of QoS.

should gracefully degrade. Finally, higher flow priorities should be given for a restricted time defined by the doctrine.

The commercial QoS in conjunction with the above listed features are jointly called Military oriented QoS (M-QoS).

It is noted that as in the case of the commercial QoS, M-QoS is also an end-to-end issue as depicted in Fig. 1. Note also that the proposed M-QoS concept does not refer to all flows that could potentially traverse a military network, but only to those which carry military essential information and require hard/soft QoS.

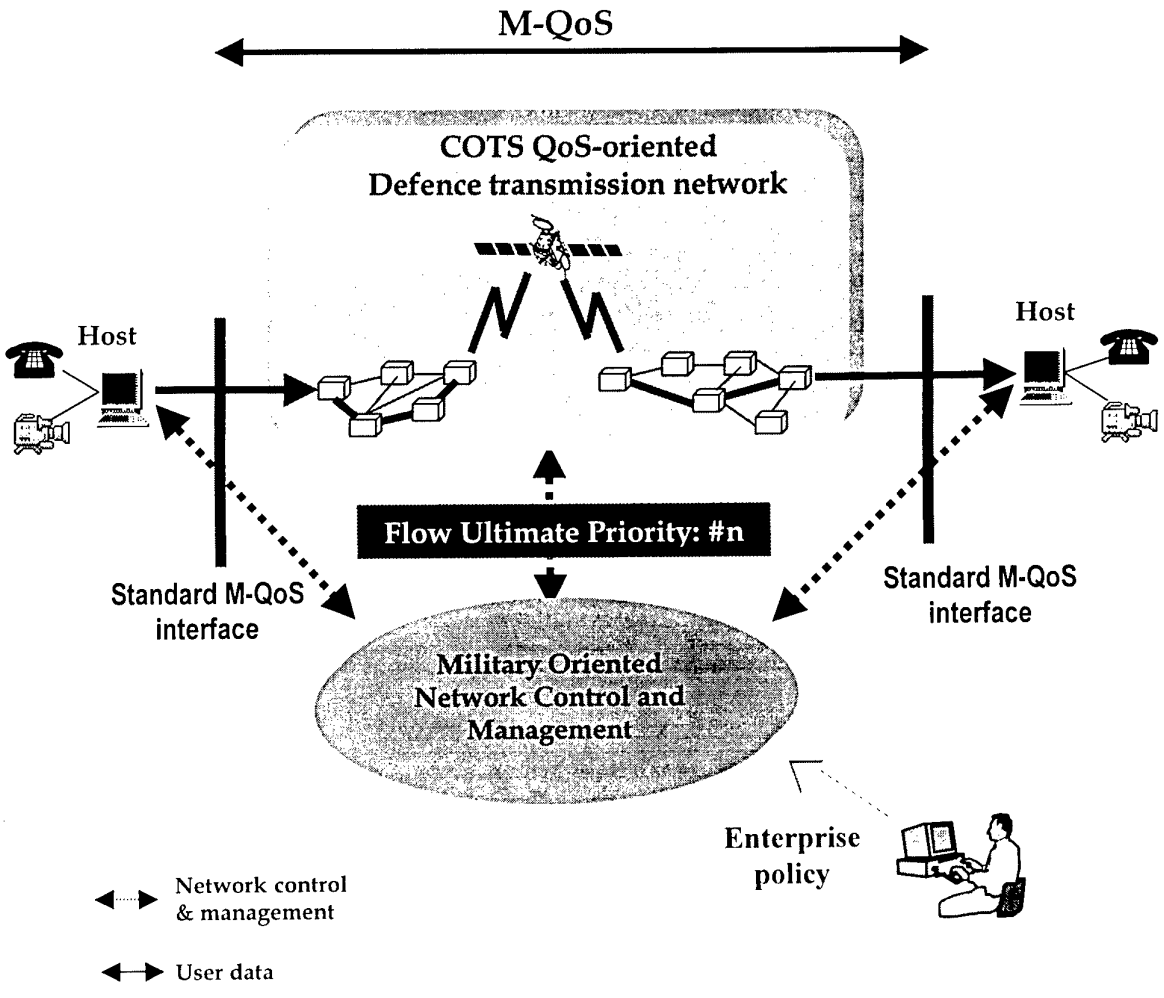


Fig. 1 The M-QoS concept.

Fig. 1 shows the basic components involved in delivering the M-QoS. These include:

a. A *standard M-QoS interface* between a military end-user application[2] and the network management and control;

   In [BLAC00a], a standard M-QoS interface within the context of policy-enabled military networks is proposed. The interface is generic in the sense that it assumes a set of commercial QoS specific (e.g., peak rate, error rate, jitter) and military specific parameters (i.e., mission identification, precedence capturing both importance and timeliness, and user perceived priority) are used to evaluate the ultimate priority of the flow according to policy(ies) currently implemented on the military network. The same interface is also used by the Military oriented Network Control and Management (see (c) below) to inform the application about any problems in delivering the requested/promised QoS.

   DSTO has developed robust software for the interface to be used in IP-oriented Defence networks

   [GEOR01].

b. *Transmission infrastructure*, which supports (commercial) hard/soft QoS features;

c. *Military oriented Network Control and Management* (M-NC&M), which:

   - Evaluates, according to a network-wide enterprise policy, the ultimate priority (UP) of the flow based on the military specific and commercial specific parameters;
   - Informs the network elements (e.g., switches, routers) how the flow should be classified and what type of preferences should be provided to it.

In summary, M-QoS can be perceived as commercial QoS with some additional military specific features.

The aims of this report are as follows:

A. Undertake a preliminary assessment of promising commercial transmission technologies in their potential support of M-QoS for a chosen subset of the Defence Core (see below);

B. Propose the best candidate(s) among these technologies for a more thorough analysis.

The report refers to short to medium term (2-5 years) design goals.

---

[2] An end-user application is understood in this report to be a software application that resides in an end-user host and interfaces with the network in order to send/receive multimedia (e.g., data, voice, video) information flows. Note that the end-user application may have an adjunct, which interfaces with network control and management on the application's behalf [GEOR01]. In this case the application only sends and receives data from the transmission network.

The subset of the long-distance Defence Core communications environment chosen for the analysis is composed of (see Figs. 2 and 3):

a. *Packet oriented fixed (terrestrial) networking infrastructure,* used for strategic communications and composed of the Backbone Routing Service (BRS), the Secure Backbone Routing Service (SECBRS) and the Defence Corporate Backbone Network (DCBN) (see [BLAC01] for details). In this report, this infrastructure will be called *fixed network* for short.

b. *Packet oriented satellite infrastructure,* used to:

   - interconnect the fixed network with a (mobile) *tactical trunk network* (e.g., used by deployed headquarters)[3];
   - provide back-up connectivity for the fixed network.

   Only geosynchronous earth orbit (GEO) satellites with bent-pipe transponder relays and no onboard processing will be considered. This is because Optus C1 and other commercial/military satellites that will most likely be used by Defence in the chosen time frame are of this type[4] [STIM01].

For the sake of simplicity, whenever the term *Core* is further used in this report, it will mean the above-specified subset of the Core. It is noted that the chosen environment is becoming crucial in carrying bulk Defence multimedia traffic.

In this report, we are interested in using the above environment for Local Area Networks (LANs)/Base Area Networks (BANs) interconnectivity. However, for both cases (a) and (b), of our interest are only network nodes (e.g., routers, switches) and control/management entities that are directly involved in long-haul transmission. The report assumes that LANs/BANs do not create any problems in providing hard/soft QoS to end-user applications due to the abundance of available bandwidth.

Within the chosen communications environment only the ATM-based DCBN offers hard/soft QoS[5]. The IP-oriented BRS and SECBRS networks only offer the best effort service.

---

[3] It is noted that other components of a tactical network such as a combat net radio sub-system are beyond the scope of this report.

[4] Although Defence may be interested in using the Iridium system, which is a low earth orbit (LEO) constellation of satellites, the system can only offer voice communication service with a very slow data transmission service.

[5] Hard QoS is achieved through the use of ATM Constant Bit rate (CBR) class of service, mainly for the voice traffic. In this case, Virtual Channel Connections (VCCs) are used to dynamically establish voice connections originating in the Defence Voice Network (DVN) [BLAC01]. Soft QoS is obtained by giving statistical preferences to different classes (i.e. aggregates) of traffic. For example, the CBR traffic gets the highest priority, the real-time Variable Bit Rate (VBR) second highest and so on.

It is noted that although the DCBN uses connections over commercial terrestrial carriers to carry traffic between ATM switches (see [BLAC01] for details), these connections are of a permanent type and this report assumes that they always provide the agreed QoS.

The structure of the report is as follows. The description of the criteria used for assessment of transmission technologies is described in Section 2. The assessment itself in regard to a set of chosen technologies is presented in Section 3. Section 4 proposes the best candidate(s) among these technologies for a more thorough analysis. The summary of the report's findings and recommendations are presented in Section 5.

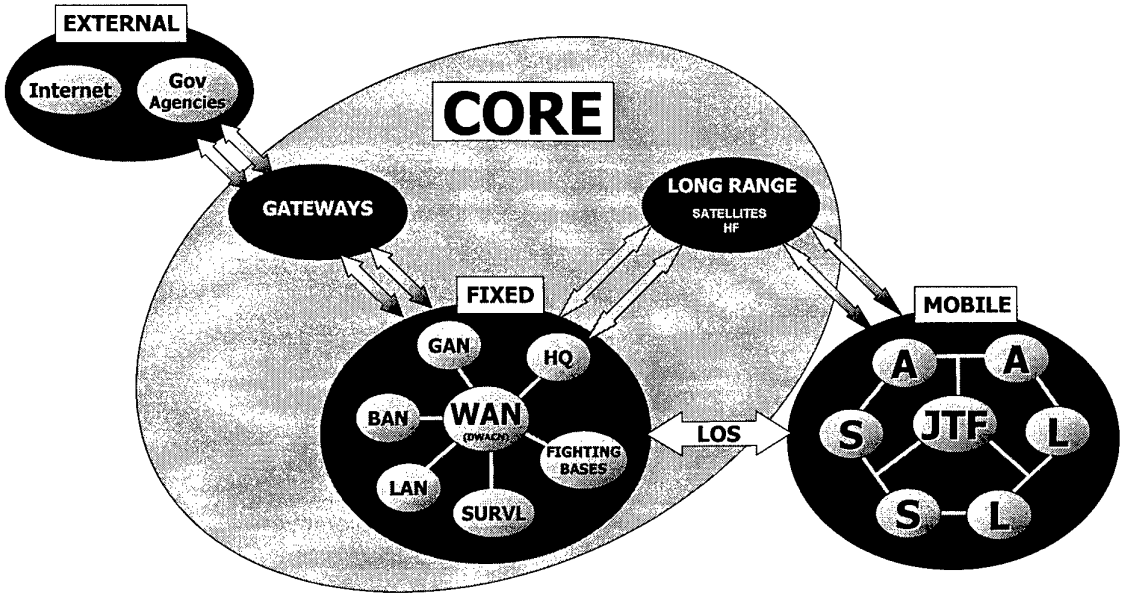


Fig. 2 Defence Core communications environment.

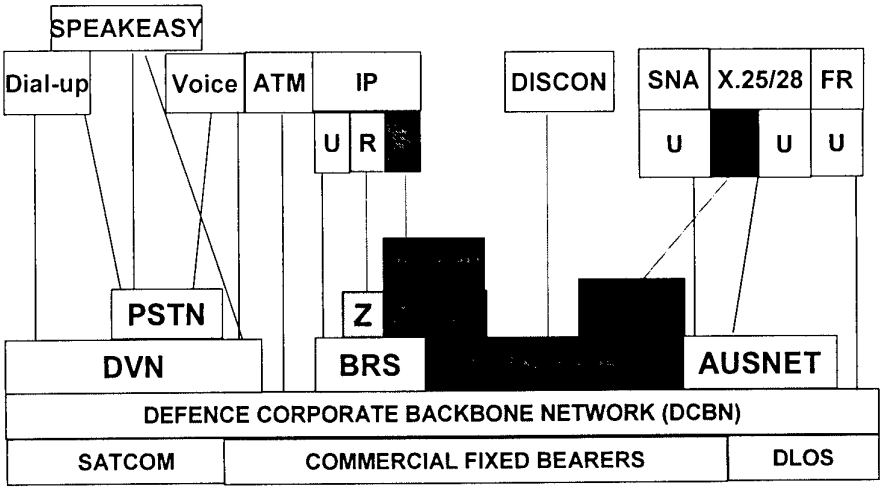


Fig.3 Basic transmission services offered by the packet Defence Core communications infrastructure [DIBE99].

2. Criteria for assessment

The various transmission technologies will be analysed in this report from the viewpoint of their provision of the following features supporting M-QoS:

A. Commercial QoS

QoS should be offered for both military specific and non-military specific flows as well as flow aggregates. The latter is important to preserve scalability in the core of a large WAN (e.g., Defence WAN), as indicated in the criterion "scalability" (see (G) below).

Note that hard QoS may not be available for some applications when slow links are used.

B. Prioritisation/preemption

Preferably, this feature should be available for both individual flows and flow aggregates. For the latter, all flows constituting an aggregate should have the same priority.

It is desirable for the network to offer mechanisms that prevent complete starvation of less important traffic when prioritisation is in use.

Note that flow prioritisation can be used not only by flow admission control, but also by network control and management to give preferences to flows/flow aggregates, for example when traffic is restored after a network failure.

C. Graceful degradation of hard QoS

Gradual stepping down in hard QoS of less important traffic should be available for both individual flows and flow aggregates.

D. QoS interface with end-user applications

The QoS interface between an end-user application and the network should enable:

- The application to specify all parameters necessary to characterise the requested QoS for the information flow;
- The application to receive a flow establishment request from a remote application;
- The application to confirm/reject a flow establishment request from a remote application;
- The network to inform the application about any problems in delivering the requested/promised QoS.

E. QoS modification

This feature enables an end-user application to request from the network a QoS modification of an already admitted flow.

F. Traffic Engineering

Traffic engineering addresses the issue of performance optimisation of operational networks [AWDU99][6]. It aims at minimising congestion due to inefficient mapping of traffic flows onto available network resources, which may result in under-utilisation of some parts of the network and over-utilisation of others.

The performance measures of interest include link utilisation, delay experienced by packets when traversing a link and the recovery time after a failure. Note that the use of the latter measure impacts on network services availability. To achieve specific thresholds for these performance objectives, network traffic has to be measured, characterised and controlled.

Constraint-based routing is a technique which can facilitate traffic engineering by finding paths satisfying certain routing policy constraints (e.g., avoidance of particular links) or QoS constraints[7] [APOS99].

G. Scalability

Since it is expected that a large number of information flows may traverse the chosen subset of the Defence Core infrastructure, it is essential to use a technology that scales well. Such technology should assure that both the control traffic and state information kept at network nodes (e.g., routers, switches) are less than proportional to the number of flows.

H. Bandwidth usage efficiency

Today's multimedia applications require a wide range of bandwidth. It is then desirable, particularly for impoverished (e.g., satellite) links, that the network technology:

- Provides fine granularity of the allocated bandwidth, thus enabling its efficient use. This applies both to individual flows as well as flow aggregates;
- Offers reserved, but not used bandwidth to less important traffic;
- Imposes small overheads;
- Offers multicasting.

---

[6] The definition of traffic engineering provided in [AWDU99] refers only to the Internet, but we extend this definition to cover any packet switching networks.

[7] This type of routing is also known as *QoS routing*.

I. Implementation in commercial networks

This feature indicates the extent to which the technology is already used in commercial (terrestrial/satellite) WANs, and if not yet, the prospects that it will be embraced by commercial industry, thus resulting in a variety of COTS products.

J. Implementation in military networks

This feature identifies the current status and plans to implement the technology in packet switched military WANs, both terrestrial fixed and satellite. The following three environments are of interest:

- The subset of the Defence Core identified in Section 1;
- The WANs used by the US DoD;
- Coalition WANs.

It is noted that features A-F above are in direct support of M-QoS. The remaining ones indirectly influence the potential of implementing M-QoS in the Defence Core.

3. Review of Transmission Technologies

The following transmission technologies have been chosen for the assessment of their support of M-QoS:

- ATM;
- IP Integrated Services (IntServ);
- IP Differentiated Services (DiffServ);
- Multi Protocol Label Switching (MPLS);
- IP Version 6 (IPv6).

These technologies are either already implemented or can potentially be implemented in the Defence Core.

In the following sub-sections, for each of the technologies, a brief description will be provided followed by assessment against the criteria described in Section 2.

3.1 ATM

3.1.1 General Description

ATM is a technology, which has been designed to efficiently support end-to-end QoS for multimedia traffic. The conceptual model of ATM is presented in Fig. 4. ATM has its own reference model, different from the OSI model and different from the TCP/IP model [TANE96]. It is composed of the ATM Adaptation Layer (AAL), the ATM Layer and the Physical Layer. The AAL is used to separate the service-independent ATM subnetwork from service specific functions. Its functions are performed at the edges of the network.

The ATM Layer is used to provide a sequential end-to-end transfer of ATM packets called cells according to the ATM protocol information contained in the cell headers [CHEN95]. The ATM cell formats at two standardised interfaces, the User Network Interface (UNI) and Network Node Interface (NNI), are shown in Fig. 5.

The purpose of the Physical Layer is to transmit ATM cells as bitstreams across a physical medium.

ATM is a connection-oriented technology using the concept of virtual connections (VCs). A number of VCs can be aggregated into Virtual Paths (VPs). VCs and VPs can be established, maintained and cancelled across the network using:

- Management Plane - this set up is static, and the connections are called Permanent VCs (PVCs) and Permanent VPs (PVPs) , respectively;
- Signalling Plane – this set up is dynamic, and enables efficient use of bandwidth; the connections are called Switched VCs (SVCs) and Switched VPs (SVPs), respectively.

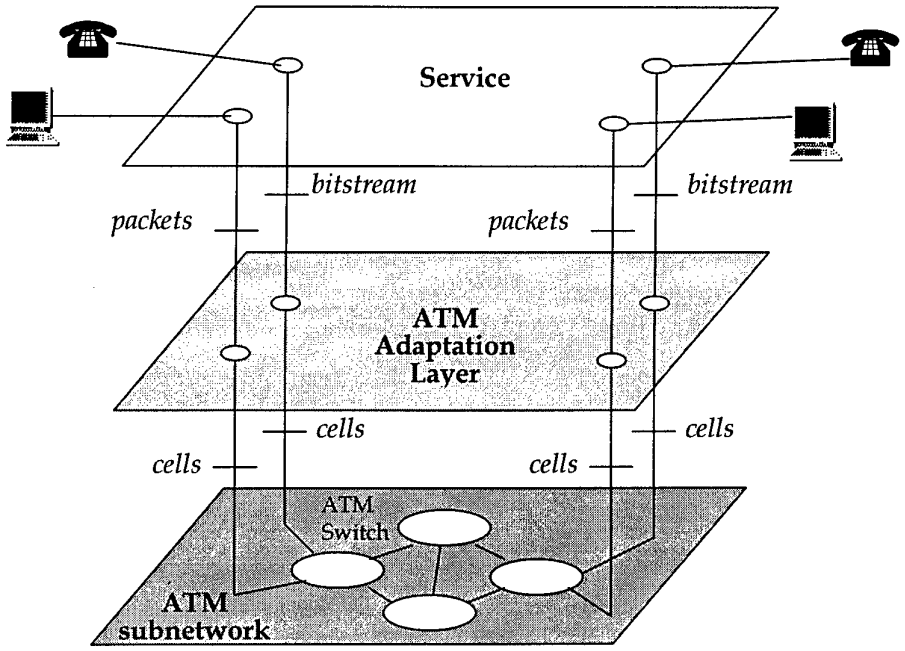


Fig. 4. Conceptual model of ATM integrating various services [CHEN95]. (The ATM subnetwork is composed of the ATM Layer and the Physical Layer.)

ATM has the potential to provide a predictable transport service for multimedia traffic, not only in terrestrial but satellite networks as well (see e.g., [IUOR99, FARS00]).

Two international bodies, the ATM Forum and the International Telecommunication Union (ITU), with its Telecommunication Standardisation Sector (ITU-T) and Radiocommunication Standardisation Sector (ITU-R), have been undertaking the ATM standardisation efforts.

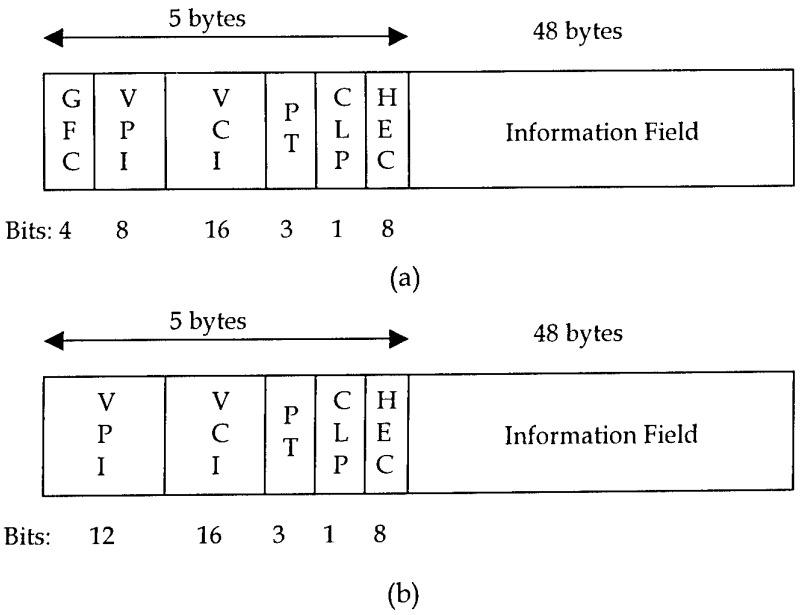


Fig. 5. ATM cell layout at (a) UNI and (b) NNI. (GFC – Generic Flow Control, VPI– Virtual Path Identifier, VCI – Virtual Channel Identifier, PT – Payload Type, CLP – Cell Loss priority, HEC – Header Error Correction.)

3.1.2 Assessment of M-QoS Support

A. Commercial QoS

ATM is a well-standardised technology providing excellent support of QoS for which it uses well-designed and understood algorithms. The ATM Forum [ATMFM96] has defined a number of service categories used to specify a traffic contract between a user and a network. These categories include:

- *Constant Bit Rate* (CBR), to support real-time applications with tightly constrained jitter (e.g., voice, constant bit video, circuit emulation);
- *Real Time Variable Bit Rate* (rt-VBR), used to carry both delay and jitter sensitive, bursty traffic, such as voice and variable bit rate video;
- *Non-Real Time Variable Bit Rate* (nrt-VBR), supporting applications which generate bursty traffic, are not sensitive to delay or jitter, but expect low cell loss ratio. Examples are Telnet and file transfers;
- *Available Bit rate* (ABR), used for non-real time applications (e.g., Web browsing), which can adjust their transmission rate depending on the feedback obtained from the network. Typical applications include FTP, WWW, and Telnet;

- *Unspecified Bit Rate* (UBR), which essentially is a best effort service, with no bandwidth, delay or cell loss guarantees. An example application is LAN emulation.

Traffic parameters (e.g., Peak Cell Rate, Sustainable Cell Rate) and QoS parameters (e.g., peak-to-peak cell jitter) are used to specify attributes of the above classes.

On the other hand, the ITU-T uses ATM Transfer Capabilities (ATCs) and QoS Classes instead of service categories. The ATC describes the ATM Layer parameters. The QoS class specifies network performance parameters (e.g., cell jitter). The ITU-T Recommendation I.356 defines four QoS classes in relation to a reference configuration covering multiple ATM networks operated by different carriers [DYSA00]. The Leaky Bucket algorithm is used to assure the conformance of the user's traffic with the traffic contract.

ATM can be utilised to offer QoS in the satellite environment. A short ATM cell size helps to achieve small jitter values for voice traffic even when sent over slow (e.g., satellite) links. However, ATM was originally designed for terrestrial fiber optic links characterised by low Bit Error Rate (BER), random bit error distribution and small propagation delays. On a satellite channel, the BER is orders of magnitude higher. In addition, errors often occur in bursts (due to variations in satellite link attenuation and the use of convolutional coding to compensate for channel noise) often leading to unacceptable cell losses. Moreover, large propagation delays are typical for GEO satellite links. These delays can reduce the effectiveness of ATM traffic and congestion control mechanisms [AKIL97].

Many research activities have led to acceptable solutions overcoming or substantially diminishing the above listed problems. The results of these activities enabled the international and national standardisation organizations to initiate, and in some cases already develop strategies addressing the issues of using ATM over satellites and the interoperability between terrestrial and satellite ATM networks[8].

B. Prioritisation/pre-emption

ATM uses the following two standardised approaches to prioritisation:

- *Class of Service (CoS) prioritisation* - this prioritisation is available at the level of ATM service classes. Cells belonging to the CBR class get the highest priority, then rt-VBR, nrt-VBR, ABR and finally UBR (e.g., see [SANT01]).

---

[8] The ITU-R has recently developed two recommendations, S1420 and 1424 [CUEV99], dealing with performance and availability of ATM over a satellite channel. The recent work of the TR34.1 subcommittee of the US Telecommunications Industry Association (TIA) on both transparent ("bent-pipe") and on-board switching has led to a new standard related to the use of ATM over point-to-point satellite links [CHIT00]. The TR34.1 is now addressing the problems of transmitting voice over ATM over satellite through studying the evolving standards and analysing their early implementations in test bed environments.

- *Cell prioritisation* – this prioritisation is offered at the level of individual cells. Two priority levels are available by setting the Cell Loss Priority (CLP) bit (see Fig. 5) in the header. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0. The CLP bit can be set by the end-user, User Parameter Control (UPC) or by a Network Parameter Control (NPC), the latter being placed at the boundary between two networks.

Note that there are no other standardised mechanisms to prioritise VCs or VPs. However, proprietary prioritisation mechanisms have been developed by vendors. For example, Lucent Technologies' PSAX 1250 switch [LUCE00] offers ten priority queues[9] per output port and Nortel switches of series 6000, 7000 and 15000 use eight priority queues per output port.

Another approach to flexible prioritisation/pre-emption of ATM VCs/VPs has been developed in DSTO and presented in [KWIA99a]. This approach is based on the use of the Generic Cell Rate Algorithms (GCRA) under direct MIB manipulation. Management Plane is used here to establish, maintain and delete flows, not signalling. Note that the GCRA is supported by a standard ATM switch at the levels of both individual VCs and VPs. The proposed solution has been verified using a demonstrator running experimental software, mainly developed at DSTO. However, to the best of the author's knowledge, there are no commercially available products utilising the GCRA for flow preemption.

C. Graceful degradation of hard QoS

Graceful degradation of hard QoS can be achieved using the GCRA algorithm under direct MIB manipulation as discussed in (B) above. It can be achieved at both VC and VP levels.

D. QoS interface with end-user applications

Both the ITU (see standards Q.2931 [Q.2931] and Q.2971 [Q2971]) and ATM Forum [ATMS96] specify signalling procedures for dynamically establishing, maintaining and clearing ATM connections at the ATM User-Network Interface (UNI). The procedures are defined in terms of messages and information elements used to characterize the ATM connection.

[9] Four of these queues are used for the CBR traffic, five for the VBR traffic, and one for the UBR traffic. All CBR queues and one VBR have top priorities. Priority queueing is used to serve the queues. That is, a lower priority queue can only be served when all higher priority queues are empty. Note that this approach may lead to complete starvation of less important traffic.

E. QoS modification

The ITU standards Q.2963 [Q2963.1], Q.2963.2 [Q2963.2] and Q.2963.3 [Q2963.3] specify how modifications of the traffic descriptor for an active VC connection can be requested across the User-Network Interface (UNI). Based on these standards, the ATM Forum proposed in [ATM0148] its own standard to modify the traffic descriptor of an active connection across the UNI, Private Network-Network Interface (PNNI) and ATM Inter-Network Interface (AINI).

F. Traffic Engineering

ATM can offer basic constraint-based routing using the Private Network-Network Interface (PNNI) signalling protocol defined by the ATM Forum [PNNI96]. A flooding protocol is used to regularly (e.g., on an hourly basis) distribute amongst nodes not only cost but also available capacity of the link. When a request for a new VC or VP arrives, the link capacity estimates are used at a source node to evaluate a path that satisfies the required capacity for the VC/VP with the least cost. The path itself is established using an explicit source routing mechanism, which specifies the entire path.

Traffic engineering can also be used to implement Permanent Virtual Circuits (PVCs). In this case, PVC paths are statically evaluated to satisfy both PVC bandwidth requirements and routing constraints, and downloaded on a regular basis [DYSA00].

G. Scalability

The use of VPs provides good scalability even for large wide area networks.

H. Bandwidth allocation efficiency

ATM enables efficient use of bandwidth by assigning it on demand and with fine granularity at both VC and VP levels. In addition, traffic streams can be statistically multiplexed, which is particularly useful in the case of bursty traffic streams having average cell rate much smaller than the link rate. However, if IP is used in the Network Layer, ATM introduces approximately a 20 % overhead.

Multicasting is available in terrestrial ATM at both the VC and VP levels. Standard ATM switches provide this functionality. As for satellite communications, the TR34.1 subcommittee of the TIA is now developing a standard for point-to-multipoint ATM Multicast over a satellite at the Physical Layer [CHIT00].

I. Implementation in commercial networks

ATM has not succeeded in being a ubiquitous broadband for all (i.e., both local and wide-area) environments in a sufficiently economical manner, but it is a solid addition to the telecommunications market [DMO00]. When implemented to the desktop, ATM

is still a costly solution. Also, the number of applications available on the market for pure desktop-to-desktop ATM connections is very limited.

Nowadays, ATM is mainly used in the core part of WANs in the form PVCs/PVPs used to interconnect edge IP routers. SVCs/SVPs are gradually being implemented to enable dynamic use of bandwidth.

In the satellite environment, few systems fully employ ATM. However, several new major GEO systems are in the planning stage, including Astrolink, Cyberstar and Spaceway [FARS00]. Most of these systems operate in Ka-band (20/30 GHz).

The problem of bursty errors (see (A) above) on satellite channels has been successfully addressed by COMSAT in its ATM Link Enhancer (ALE-2000) and Link Accelerator (CLA-2000/ATM). These products provide an essentially error-free satellite link in a bandwidth efficient manner for a wide range of rates [CHIT00].

J. Implementation in military networks

J.1. ADF perspective

ATM has been used for a longer time in the Defence terrestrial WAN in a similar fashion as in large commercial networks, that is to create a high capacity backbone, called DCBN (see Fig. 3) which switches voice, video and data within the Core infrastructure. Nortel's Passport switches are used for this purpose. The service is offered mainly to the Defence Voice Network (DVN) and the Backbone Router Service (BRS). 155 Mbit/sec access ATM links, in the form of both real time and non-real time VCs, are used. The VCs are aggregated into VPs when transiting Telstra and Optus ATM networks [BLAC01]. The currently pending Phase 1A of JP 2047 (DWACN) aims at upgrading the core of the Defence WAN and assumes the use ATM for a foreseeable future [ADVA00].

In the Defence satellite environment, the use of ATM over the Optus C1 geostationary satellite for multimedia communication between tactical trunk networks and the fixed network is currently considered by JP2008 Phase 3E. One objective is to support Project Parakeet (JP65), where ATM is planned to carry circuit switched and IP traffic for the Battlefield Command Support System (BCSS) [BLAI01]. It is noted that DSTO is currently analysing the impact of errors in the satellite environment on ATM capabilities sought by Defence [WILK01].

J.2. US DoD perspective

ATM is a key transport technology of the National Information Infrastructure and the information infrastructure of the Department of Defence for supporting voice, video, data and multimedia services [VAKI98, HADJ98, SHVO98, ELMO98]. Originally, ATM was perceived as the preferred end-to-end technology for *Command, Control, Communications, Computer and Intelligence* (C^4I) systems [BOWM98], but the push towards IP technology at the network edges is visible.

J.3 Coalition perspective

The author is aware only of one example of the planned use of ATM in a Coalition environment, that is in the Combined Federated Battle Laboratories Network (CFBLNet)[10] to carry aggregates of IP flows [CFBL00].

[10] CFBLNet is a coalition research network currently built by the US Joint Battle Center (JBC) by making the existing temporary Joint Warrior Interoperability Demonstration (JWID) network a permanent network [LEPP00]. CFBLNet is perceived as a precursor to an operational Coalition Wide Area Network (CWAN).

3.2 IP Integrated Services

3.2.1 General Description

The Integrated Services (IntServ) is a Network Layer technology designed by the IETF in the mid 90s to provide QoS for Internet applications. IntServ is a technology which guarantees service to each traffic flow in isolation from other traffic flows [BERN00a]. Data flows are identified by the 5-tuple (source IP address, source port, destination IP address, destination port and used Transport Layer protocol (e.g., TCP, UDP)). When a flow is to be established, a set of QoS requirements is passed to the network, including bandwidth, maximum packet delay and packet loss. No fragmentation of packets is allowed [WHIT97]. The network tries to reserve sufficient resources in routers in order to satisfy the requirements. A signalling protocol called Resource Reservation Protocol (RSVP) [BRAD97, WROC97a] has been designed to reserve the resources in the network and to exchange control information with the applications.

When a flow is to be established, an RSVP Path message (see Fig. 6) is sent from the sender to one or more destinations (i.e., in the case of multicasting). This message contains characteristics of the traffic flow, which include peak rate of the flow, token bucket rate corresponding to the sustainable (average) bandwidth of the flow, bucket depth describing how much data rate can exceed the sustainable rate, minimum policed packet size, and maximum policed packet size. In the case of the Guaranteed Service class (see next section), the Path message also includes characteristics of the source of the flow and routers traversed by the message. These characteristics are then used by the receiver(s) to evaluate the actual end-to-end QoS requirements, such as total delay and bandwidth. These are included in the Resv message sent back (using the same path as for the Path message) to the sender, and all routers along the path try to reserve the required resources.

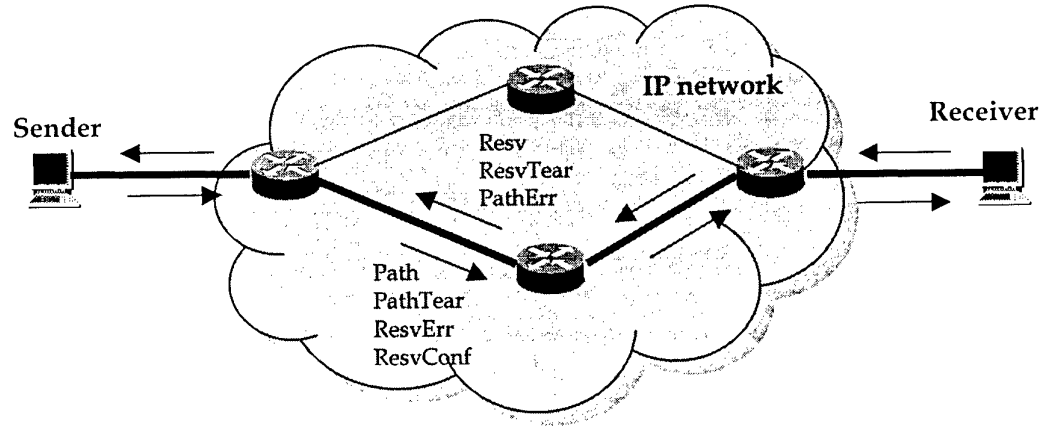


Fig. 6. RSVP messages.

The RSVP is required to periodically update path states in all the routers along the path of the flow. In other words reservations are "soft", as opposed to "hard" reservations used for example by ATM (see Section 3.1). The reservation remains valid until an application explicitly requests its termination or the network signals the application that it is not able to maintain the reservation.

RSVP, which is a fairly complex protocol, is normally implemented in end-user hosts to provide the end-to-end provision of IntServ.

3.2.2 Assessment of M-QoS Support

A. Commercial QoS

Two service classes have formally been specified for IntServ by the IETF, namely [DYSA00, SHEN97, WHIT97, WROC97b]:

- *Guaranteed Service (GS) class*

  This class provides hard QoS similar to circuit reservation since it offers a guaranteed bandwidth, (mathematically proven) deterministic upper bounds on end-to-end packet delay and jitter, and no queueing loss. This class is intended for real time applications such as audio and video.

- *Controlled-load Service (CS) class*

  This class does not guarantee firm QoS, but only provides an equivalent of best-effort service under lightly loaded conditions. It is suitable for applications, which can tolerate some packet loss and delay, such as adaptive real-time applications (e.g., H.323 traffic).

A token bucket algorithm is used to police user traffic and mark non-conforming packets [DYSA00]. This algorithm is also applied to smooth the data flow. For both GS and CS classes, the non-conforming traffic is usually treated as best effort [STAR99].

With IntServ, the routers are responsible for negotiating relevant QoS requirements with the Link Layer devices such as ATM switches.

IntServ is asymmetric in the sense that only the receiver, not the sender, actually specifies the requested QoS.

B. Prioritisation/pre-emption

RSVP version 1 does not allow for any explicit flow prioritisation. If there are not enough free resources, the request to establish a flow is refused. Recently, however, some aspects of flow prioritisation have been included in RSVP extensions to policy-based admission control [HERZ00a, HERZ00b, YAVA00]. These extensions are used to monitor, control and enforce the use of network resources according to a policy centrally stored in a Policy Decision Point (PDP) [CHIU99]. An important criterion of

the policy is the rank of the flow importance expressed by *preemption priority*. It is used to select a flow of highest priority, even if this would require preempting already admitted (lower priority) flows. For the latter, the preempted flows are deleted. Once a flow is admitted, the preemption priority is replaced by *defending priority* (of a higher value), which is then used to compare with preemption priorities of new flows.

C. Graceful degradation of hard QoS

As stated in (A) above, hard QoS can only be achieved with the GS class. The network cannot, however, gracefully degrade the promised QoS. If the network is not able to guarantee the reservation, the connection is cancelled.

D. QoS interface with end-user applications

End-user applications use the RSVP interface with the network usually in the form of an API. This interface enables the sender to specify the required class of IntServ (i.e., GS or CS) and traffic description, while the receiver uses it to specify the required QoS specification. The receiver is informed when the network rejects the requested QoS and service class. Note that the receiving application can use RSVP to inform the sending application about its receiving capabilities.

For the GS class, the receiver is also informed about any problems that network may have in delivering the agreed QoS, for example as a result of preemption by another flow.

E. QoS modification

A modification to QoS requirements can be invoked by the receiving end-user application for a GS class connection. This results in a new QoS request when a periodical update of soft reservation states is performed in routers. The request may be accepted or rejected, resulting in the connection cancellation for the latter.

F. Traffic Engineering

Since RSVP is a signalling, not a routing protocol, it has to rely on the routing protocols available at the Network Layer. RSVP can be complemented with traffic engineering, which decides the chosen paths through the network. If traffic engineering is not used, some form of route pinning has to be applied to assure that the route of the Path message will be used by all subsequent messages of the same flow (see Fig. 6).

G. Bandwidth usage efficiency

The use of RSVP by IntServ provides an efficient mechanism to reserve bandwidth with fine granularity. IP packets are transmitted without any overheads. The signalling

traffic related to a flow establishment and cancellation is small. However, the need for periodic updating of soft states may create a considerable signalling traffic overhead if a large number of IntServ connections are present. This feature may be important when considering the use of RSVP over low capacity (e.g., satellite) links.

Note that RSVP has been designed to support efficient multicast traffic.

H. Scalability

RSVP version 1 lacks facilities to aggregate individual flows. This results in processing and memory requirements being proportional to the number of flows, which, in conjunction with the need to periodically update soft states, may create a real scalability problem in a wide-area network with a large number of IntServ flows. On the other hand, multicasting even with a considerable number of receivers, scales very well with RSVP [CHIU99].

It is noted that extensions to RSVP enabling aggregate reservations are being discussed by the IETF [BERN00, BAKE00].

I. Implementation in commercial networks

IntServ is a matured, well-standardised technology. The vast majority of IP routers support it. As for the provision of RSVP in hosts, Microsoft supports it in its Windows 2000 operating system [PETR99]. It is also readily available for Unix operating systems.

However, due to its scalability problems, it is very unlikely that IntServ will be used in its current form to provide end-to-end QoS on a large scale in terrestrial WANs. Whether the extensions enabling aggregate reservations (see (H) above) will be sufficient to change the role of IntServ, is yet to be seen. Meanwhile, the use of IntServ has been considered recently in conjunction with DiffServ (see next section). In this scenario, DiffServ, being much more scalable but not designed to interface with end-user applications, is used in the core part of a terrestrial WAN. IntServ is then utilised to interface end-user applications with the DiffServ-enabled core (see [WROC01] for details).

The author is not aware of any attempts of using IntServ over satellite links. Since the realistic number of flows over a satellite link is usually much smaller than for a terrestrial counterpart, scalability may not be a significant issue. However, the impact of bandwidth overheads caused by RSVP signalling traffic on satellite links due to soft updates requires investigation.

J. Implementation in military networks

J.1. ADF perspective

Although IP routers in the Defence Core are capable of offering RSVP, to the best of the author's knowledge no attempts have been made to offer IntServ to Defence customers.

J.2. US DoD perspective

Although the US DoD's strategic network (DISN) does not offer IntServ, a couple of experiments involving this technology have been recently reported. One such experiment is presented in [MIRH00], where a variation of the RSVP (called dRSVP) is used to provide QoS in a dynamically changing network environment, such as a tactical wireless LAN. Rather than making a binary "admit/fail" decision for each flow, a typical approach used by RSVP, the network provides feedback to applications on the current reservation level thus allowing them to adjust to the available QoS level. The authors propose a number of additions to the standard RSVP to support the concept of reservation changes. However, there are no indications that the IETF will attempt to include the additions into the existing RSVP standards.

J.3 Coalition perspective

The author is not aware of any plans to use IntServ in a Coalition environment.

3.3 IP Differentiated Service

3.3.1 General Description

The scalability problems of IntServ forced the IETF to propose a different technology called Differentiated Services (DiffServ) [BLAK98]. It is also a Network Layer technology, but as opposed to IntServ, it uses a simple and a coarse method of classifying packets requiring similar QoS into a limited number of Classes of Service (CoS). All packets to be transmitted over the same link and requiring the same DiffServ behaviour constitute a Behaviour Aggregate (BA).

A DiffServ network is divided into domains as depicted in Fig. 7. A domain is usually controlled by a single entity, such as an Internet Service Provider (ISP). DiffServ is extended across domains through the use of Service Level Agreements (SLAs) between pairs of these domains [STAR99]. SLAs are complex business-related contracts describing network availability guarantees, payment models, legal specifics etc. [TEIT99]. Note that SLAs are also used between end-users and a network. A Service Level Specification (SLS) is a part of an SLA contract describing QoS aspects. The specification of an SLS, the configuration of a domain's edge routers and flow admission control can be done either manually or can be automated, the latter being particularly valuable if the number of flows is large and the SLS are not static.

Typical functions performed by routers include packet classification, marking, metering, shaping, dropping and scheduling. Packet marking is performed using DiffServ Code Points (DSCPs) corresponding to their BAs. The maximum number of code points is 64. The DSCP format is presented in Fig. 8. For IPv4, the marking is accomplished using the Type of Service (TOS) octet in the header. The first three bits of

the octet are called the IP Precedence bits. In the case of IPv6, DSCPs are specified by the Traffic Class octet. In each router, the DSCP of an incoming packet is used to choose a per-hop-behaviour (PHB) which determines the forwarding behaviour the packet will experience in the router. PHBs are implemented in routers through some (not standardised) packet scheduling and dropping mechanisms.

The Traffic Conditioning Agreement (TCA) specifies classifier rules and any corresponding traffic profiles and metering, marking, dropping (also called policing), and shaping rules [BLAK98].

Different types of routers can be distinguished depending on the position in the network (see Fig. 7). Ingress Routers (IRs) ensure that the traffic entering the domain from user hosts conforms to the agreed SLSs. To perform this function, an IR uses packet classification, packet marking and policing on a per flow basis. Transit Routers (TRs), also called core routers, perform classification on aggregates. The main purpose of Boundary Routers (BRs) is to police on packet class aggregates. Finally, Egress Routers (ERs) perform shaping of the traffic forwarded to adjacent domains, according to the agreed SLSs. Note that ingress and egress routers are also called edge routers. Note also that a single router may perform functions of different router types at the same time.

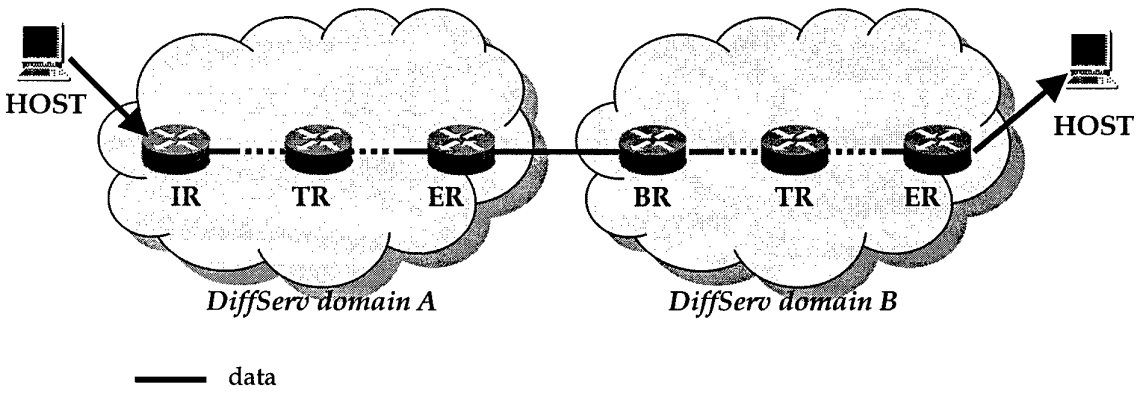


Fig. 7. DiffServ framework (IR – ingress router, TR – transit router, BR – boundary router, ER – egress router.)

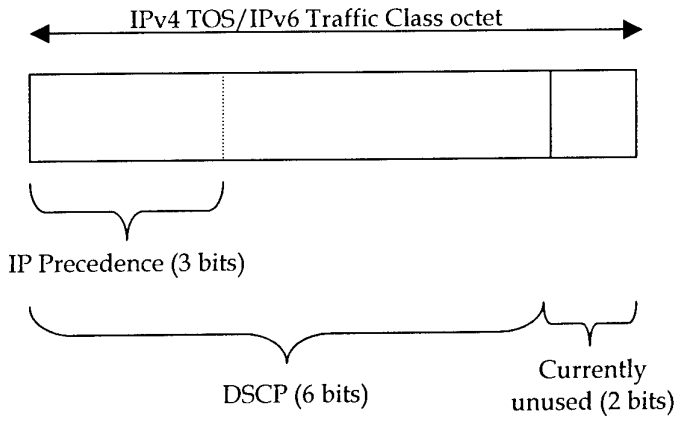


Fig. 8. Differentiated Service Code Points.

A special entity called a *Bandwidth Broker* (BB), shown in Fig. 9, can be used to facilitate automatic SLS arrangements [TEIT99]. A BB performs admission control of flows requested by end-user applications. It is also responsible for the proper provision of bandwidth within its home DiffServ domain and between domains. BBs keep information about all SLSs related to their domains. To perform flow admission control, BBs need to monitor the utilisation and health of resources (e.g., links, routers) in their domains. Note that flow admission is scalable since only the ingress router is involved in flow admission. Apart from flow admission, BBs can also configure routers in their domains. This is done infrequently and typically on a per class basis, thus ensuring that the whole process is scalable.

There can be a number of approaches to bandwidth brokerage implementation. The most advanced one has been investigated within the Qbone initiative[11] [TEIT99, QBONE]. According to this approach, a BB authenticates a flow request and then assesses whether the flow can be admitted based on the amount of resources available in the home domain and in other domains if a multi-domain reservation is required. For the latter case, the request has to be sent (using some form of inter-BB communication – see Fig. 9) to all peer BBs of the involved domains.

[11] Qbone is an international Internet initiative that aims at building a testbed for interdomain IP DiffServ.

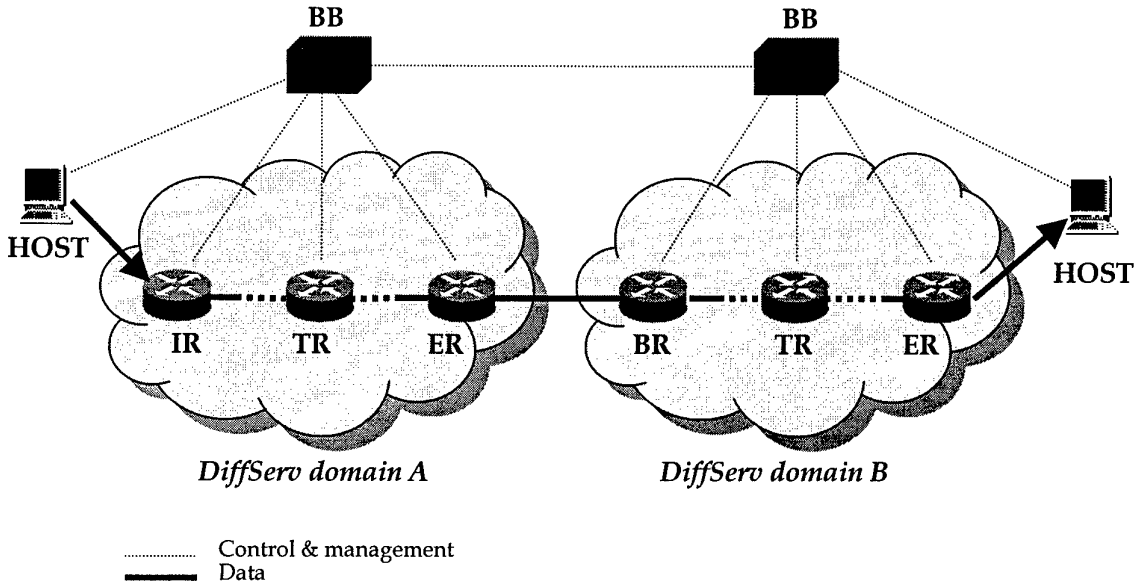


Fig. 9. DiffServ supported by bandwidth brokerage. (IR – ingress router, TR – transit router, BR – border router, ER – egress router, BB – Bandwidth Broker.)

The problem of how communication should be organised between a BB and other DiffServ network entities is currently being addressed by the Internet2[12] QoS working group [TEIT99], which considers bandwidth brokerage as an important mechanism to provide QoS in the future Internet. They propose to use SNMP, COPS or any other network management protocol for the communication between a BB and a router. The use of RSVP is being considered for the communication between a BB and a host. Finally, a specially designed protocol, called Simple Interdomain Bandwidth Broker Signalling (SSIBS) [QBONEa], is planned for communication between BBs.

DiffServ is asymmetric, that is only the sender controls the traffic class. The flow of data is unidirectional. It is expected that DiffServ will be supported by various Link Layer technologies, such as ATM and MPLS.

3.3.2 Assessment of M-QoS Support

A. Commercial QoS

The following three PHB types have been already standardised and often implemented in IP routers:

[12] Internet2 is a collaborative effort to develop advanced Internet technology and applications for research and higher education [INTE201].

- *Default PHB*

  This PHB corresponds to best effort behaviour typical for non-DiffServ routers [NICH98]. If no other agreements exist within the domain, it is assumed that all packets belong to this PHB.

- *Expedited Forwarding (EF)*

  This PHB has been designed to provide the highest QoS, which offers low delay, low jitter, low loss and assured bandwidth by (almost) precluding any queueing at routers, regardless of the load they experience [JACO99]. This PHB guarantees a minimum bandwidth and has the highest priority among PHBs. It can be used to support applications requiring nearly a constant bit rate, for example Virtual Leased Lines (VLLs) [CHIU99]. The SLS specifies the peak rate. Any traffic that exceeds the traffic profile defined by the SLS is discarded as a result of strict policing, which is performed on a per flow basis [EICH00]. Note that the EF PHB can be implemented in many ways (e.g., using priority queueing, weighted round robin queueing) [JACO99]. Deploying EF requires strict policing and shaping in all routers implementing this service to avoid situations when the arrival traffic is larger than the minimum departure rate.

  A potential problem may appear when EF is used to carry low jitter traffic, such as voice, over relatively slow links. In this case, when an EF packet has to be sent, its immediate transmission may be blocked by a long packet whose transmission has just started. Such situations may create jitter unacceptable for voice. Various solutions have recently been analysed to overcome this problem, for example using fragmentation of large IP packets and IP header compression (for the latter, see [CASN99]).

- *Assured Forwarding (AF)*

  The AF PHB defines four classes, each having three levels of drop precedence [JACO99, HEIN99]. Excess traffic is less likely to be delivered, but not automatically discarded. In each router, the four classes are allocated a certain minimum amount of resources, such as bandwidth and buffers. In the case of congestion, each class is treated separately, and within a given class the higher the drop precedence, the higher probability of the packet being dropped. A router should minimise long-term congestion within each class, while allowing short-term congestion resulting from bursts. Moreover, if congestion appears, the used dropping algorithm should treat all packets belonging to the same class and dropping (precedence) level equally. It is an implementation issue as to how the dropping mechanism is used and excess resources (if any) are divided between the AF classes.

  Note that the AF classes do not impact delay and jitter. Note also that AF classes provide relative service levels and they neither guarantee a consistent rate nor a fair share of the excess traffic [CHIU99].

The relationships between the default, AF and EF classes, such as the division of resources amongst these classes, are not standardised and left to the implementation. More PHBs are expected to be standardised in future. Meantime, the routers can be configured to apply some proprietary treatment to the not-yet-standardised DSCPs, according to some form of agreement between the network and the end-user.

As for IntServ, the routers implementing DiffServ are responsible for negotiating relevant QoS requirements with the Link Layer devices such as ATM switches.

B. Prioritisation/pre-emption

Prioritisation can only be accomplished in relation to different DSCP code points representing flow aggregates. In other words, it is not possible to allocate different priorities to two flows belonging to the same code point. The mapping between code points and priorities is generally an implementation issue. However, in the case of the code points representing different drop out probabilities within the same AF class, the prioritisation is already specified.

As stated in Section 2, it is preferable to avoid complete starvation of a class bandwidth. To achieve this requirement, Cisco has recently proposed a scheduling mechanism, called Class Based Weighted Fair Queueing, which offers up to 64 DiffServ classes (corresponding to DSCP codes) and guaranteed minimum (configurable) bandwidth per class [CISC00].

C. Graceful degradation of hard QoS

As stated in (A), hard QoS is provided by the EF service, but it can also be offered in a propriety fashion for other, not yet standardised DSCPs. The basic DiffServ architecture assumes the use of policing in relation to particular flows or their aggregates. Hence, the graceful degradation of hard QoS can be achieved by imposing throttling of selected flows/flow aggregates and thus giving preference to more important flows. Bandwidth Brokers are entities that can enforce such throttling.

D. QoS interface with end-user applications

DiffServ does not provide any standardised signalling mechanisms to specify QoS requirements by the end-user application [HUST00, TEIT99]. However, the application may indicate to the network the required QoS using one of the following methods:

- *By setting appropriate DSCP bits.*

  This method implicitly indicates to the network the requested QoS, which refers to individual packets rather than flows. Note that the end-user application cannot be informed in a standardised way about any problems (e.g., resulting in the network's or receiver's inability to cope with traffic flow) in delivering the required service level.

- *Through communicating with a Bandwidth Broker (BB).*

  This approach assumes the use of bandwidth brokerage as described in Section 3.3.1. As stated there, a signalling protocol (e.g., RSVP) can be used for the communication. Note that the BB is capable of informing the application whether the requested flow has been admitted or not.

- *Using IntServ in edge routers and DiffServ in transit routers.*

  This approach recently proposed in [WROC01] assumes the use of some form of standardised mapping between IntServ and DiffServ. More standardisation work is required to define such a mapping.

E. QoS modification

QoS modification can be achieved by an end-user application using one of the following methods:

- Through changing the setting of DSCP bits;
- Sending the appropriate request to the BB, if bandwidth brokerage is in use.

The former method allows the application to mark some or all packets of a flow thus indicating to the network a need to change QoS, but does not allow the network to inform the application whether the requested QoS is met. The latter method refers to whole flows and enables the application to obtain such feedback.

F. Traffic Engineering

DiffServ depends on the available routing options. If traditional IP routing is used, based on the Interior Gateway protocols, such as Open Shortest Path First (OPSF) or Intermediate System - Intermediate System (IS-IS), traffic engineering is difficult. This is because these protocols route the traffic within the Internet domains using a static approach based on previous traffic forecasting. Each router of a domain makes routing decisions independently. Moreover, whenever a path is to be chosen, only the shortest paths are selected, using simple additive link metrics. Although this approach is highly scalable and can be distributed [AWDU99], it has a major drawback: only the network topology is taken into account when calculating the path which in rich-connected networks may lead to under utilisation of some network links and over utilisation of others.

However, traffic engineering can be applied to IP traffic if the so-called *overlay model* (based on ATM or Frame Relay implemented in Layer 2) or MPLS (see Section 3.4) are used [AWDU99b].

G. Scalability

The scalability of DiffServ is very good since the number of states to be remembered in each router is proportional to the number of DSCP classes. Also, the use of bandwidth brokerage should not create any major scalability problems since:

- BBs are not involved in flows which require best effort service;
- Only edge routers need to be contacted by BBs on per flow basis;
- The amount of processing required for a BB to communicate with end-user applications and with other BBs can be diminished by scaling down the size of the domains and through a distributed implementation of BBs. An example of the latter approach can be found in [STEL99].

H. Bandwidth usage efficiency

If DiffServ is used alone, the utilisation of bandwidth is that offered by IPv4/IPv6. In other words DiffServ does not impose any additional overheads once configuration is completed. Note that IP/TCP [JACO90] or IP/UDP [CASN99] header compression algorithms can be used to improve bandwidth efficiency for low speed serial links.

If bandwidth brokerage is used in addition to DiffServ, additional overheads due to host-to-BB, BB-to-edge-router and BB-to-BB communications have to be taken into account. These overheads may be of some concern when slow satellite links are used. No publications addressing this problem are available to the author at the time of writing.

I. Implementation in commercial networks

Although IETF is very active in the area of DiffServ standardisation, this technology is still in the early stages of its development. The lack of a standardised interface with end-user applications certainly slows down wide implementation of DiffServ. Nevertheless, all major vendors of routers try to implement the agreed DiffServ standards.

Many commercial carriers are considering offering the standardised DiffServ services. For example, Telstra plans to offer them as part of its Data Mode of Operation (DMO) [DMO00]. A proposal of how the AF can be implemented in an experimental network is given in [CANS99][13].

A crude form of bandwidth brokerage in conjunction with DiffServ and general Policy based Network Management is already offered by some vendors, such IPHighway [IPHY01]. More such solutions can be expected in the near future due to a strong

[13] The network offers to the residential end users connected to an Access Concentrator the four AF classes being used to carry Voice over IP (first line), Voice over IP (second line), Video over IP and the best effort service.

commitment of the Internet2 to the development and experimental deployment of bandwidth brokerage (see Section 3.3.1).

The implementation of DiffServ in a satellite environment should be quite straightforward, particularly for fast satellite connections. For slow connections, two potential problems may appear. The first one (already discussed in (A)) is the problem of carrying voice over IP over slow satellite links, where unacceptable jitter may appear. The second problem refers to the signalling overheads when bandwidth brokerage is used (see discussion in (H)). The author is not aware of any study addressing this problem.

J. Implementation in military networks

J.1. ADF perspective

DiffServ is not yet offered in the Defence communications infrastructure. However, Defence's Information Systems Division (ISD) is considering undertaking experiments to assess the usefulness of this technology to the terrestrial part of the Core infrastructure [HUNT01]. The use of DiffServ in the terrestrial part of Defence Core is also anticipated by JP 2047 [ADVA00]. It is noted that in both cases the use of bandwidth brokerage is not considered.

J.2. US DoD perspective

The US Defense does not yet offer DiffServ in its strategic DISN network. There are, however, plans to investigate its use in financial year 2001 as a part of the CINC 21 Advanced Concept Technology Demonstrator (ACTD) [ODON00a].

The Mitre Corporation, undertaking research for the US DoD, has proposed a methodology of using extensions to DiffServ to enable a precedence scheme which minimises the probability of mission-critical flows being rejected or negatively affected by less important traffic [KING00]. To achieve the goal, a two level hierarchical queuing and scheduling algorithm has been designed, which provides preemptive precedence between traffic flows of different importance (e.g., flash, immediate, routine) and different traffic types (e.g., voice, video, data). Although the proposed approach is close to the M-QoS concept, it is characterised by a rigid preemptive priority scheduler that guarantees network resources be available to high precedence traffic. The approach may lead to complete bandwidth starvation of the lower precedence traffic. There is no IP router vendor offering the proposed two-level scheduling mechanism.

J.3 Coalition perspective

The use of DiffServ is planned for the core and edge IP routers of the Combined Federated Battle Laboratories Network (CFBLNet) [CFBL00]. The CINC21 ACTD is also considering the use of DiffServ in the coalition extensions of its network.

3.4 MPLS

3.4.1 General Description

Traditional IP routing does not support efficient traffic engineering. To overcome this problem, Multi Protocol Label Switching (MPLS) has been recently proposed by the IETF. As the name suggests, it is protocol-independent, and in fact can be used by various network protocols. In this report, it is assumed that MPLS is used by IP. In this section, we describe only those MPLS properties that are recognised by IETF as matured, although not necessarily yet standardised.

MPLS is a connection-oriented technology that integrates the Link Layer and the Network Layer. Its architecture is described in [ROSE01]. A set of contiguous routers, which implement MPLS-type routing and forwarding, is called an *MPLS domain* (see Fig. 10). MPLS allows for reserving bandwidth and choosing explicit, not necessarily shortest paths across the network. In this way, the total network traffic can be better balanced across all available routes.

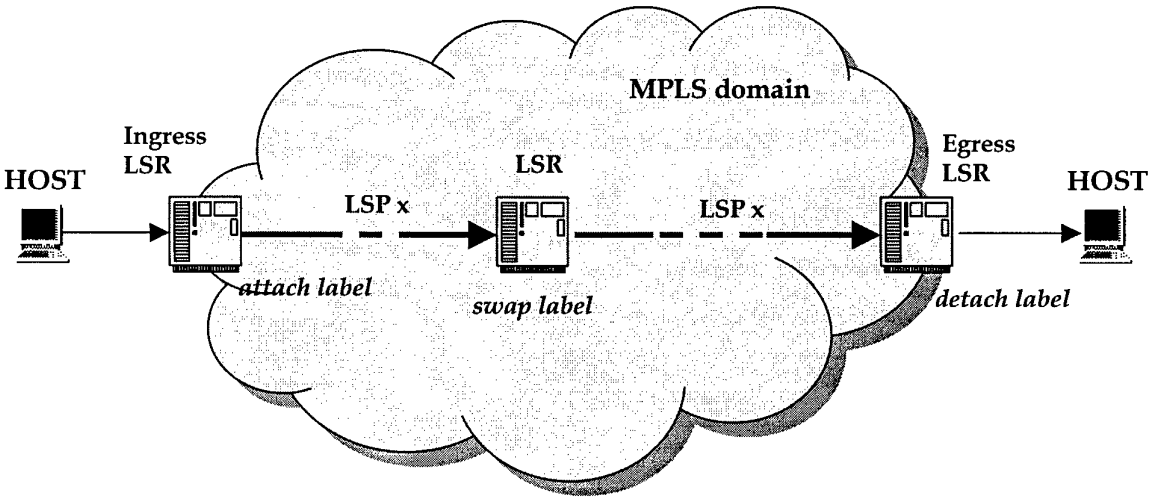


Fig. 10. MPLS domain.(LSR – label switch router, LSP – label switched path.)

LABEL (20 bits)	EXP (3 bits)	S (1 bit)	TTL (8 bits)

Fig. 11. MPLS shim header. (EXP – experimental field, S – stack indicator, TTL - time to live field.)

To achieve the above properties, MPLS utilises label switching of IP packets instead of traditional routing. As depicted in Fig. 11, a label is 20 bit long and is a part of the 32-bit MPLS header that precedes an IP packet. Label switching is carried out in special routers, called Label Switching Routers (LSRs), where packet forwarding between LSRs is done by a single index look-up into a switching table, using the carried MPLS label and, possibly, the arrival port identifier [ARMI00]. This forwarding is performed on a per-hop basis. Each label is related to a particular Forwarding Equivalence Class (FEC) representing packets forwarded in the same manner (i.e., over the same path and with the same treatment [CALL99]). Labels have local significance in the sense that the relationship between them and FECs is agreed only between pairs of communicating LSRs. Distribution of labels can be provided by various protocols, including Border Gateway Protocol (BPG), RSVP and Label Distribution Protocol (LDP), the latter two are the most likely to be used.

Apart from a label, the MPLS packet header contains a 3-bit experimental field, a 1-bit label stack indicator, and an 8-bit time-to-live field.

The path taken by a packet traversing an MPLS domain is called a Label Switched Path (LSP) (see Fig. 10). It is unidirectional, it starts in an ingress LSR, traverses one or more core LSRs and finishes in an egress router. Only the first LSR on the path analyses the IP packet's header and assigns a label. All other LSRs on the LSP only swap labels. MPLS allows an arbitrary number of labels to be stacked, which is a powerful mechanism to construct Virtual Private Networks (VPNs) as well as to enable fast traffic recovery through rerouting [SWAL99].

Each LSP can be assigned one or more of the following attributes [AWDU99b]:

a. *Traffic parameter attributes* – capturing the characteristics of the FEC, including peak rate, average rate, permissible burst size etc.;

b. *Generic path selection and maintenance attributes* – defining the rules for selecting the route taken by a LSP as well as for maintaining the already established paths;

c. *Priority attribute* – describing the relative importance of LSPs. It can be used to determine the order in which LSPs are established or restored after a fault;

d. *Preemption attribute* – deciding whether a new LSP can preempt already established ones if not enough resources are available on the route. This feature enables traffic prioritisation;

e. *Resilience attribute* – describing the recovery policy (if required) for an LSP under fault conditions;

f. *Policing attribute* – determining the actions, which should be taken when the real traffic carried by an LSP does not comply with the contract specified by traffic parameter attributes (see (a)).

Two types of LSPs are distinguished from the viewpoint of the way they are established:

- *Control-driven* LSPs (also known as *hop-by-hop* LSPs)

  These LSPs are established hop-by-hop using forwarding tables in routers, that is choosing the path normally used for typical IP routing.

- *Explicitly-routed* LSPs (also known as *Constrained-based Routing Label Switched Paths* (CR-LSPs)).

  These LSPs are set up following a path explicitly specified in the path setup message. The route of a path can be set either manually or automatically[14] taking into account the attributes (a-f) as well as the constraints imposed by the current status of the links and the administrative policy [GHAN99].

3.4.2 Assessment of M-QoS Support

A. Commercial QoS

MPLS is not designed to directly offer QoS to end-user applications. Instead, its role is rather perceived inside the network where it can significantly enhance the ability of other transmission technologies to provide QoS. Generally, there are the following two different ways MPLS can provide this enhancement:

- *Offering different LSPs for different classes of traffic.*

  Using this approach, hard QoS can be offered to flow aggregates. Mission critical flows can use LSPs traversing a small number of label switches (hence minimising total delay). Also, back-up LPS can swiftly be utilised to reroute high priority traffic after network failures.

- *Offering different Classes of Service (CoS) for the same LSP.*

  In this case, the 3-bit Experimental Field in the MPLS header (see Fig. 11) can be used to distinguish up to eight different Classes of Service (CoS) within the same LSP, thus providing soft QoS.

B. Prioritisation/pre-emption

Prioritisation can be applied at two levels of traffic aggregates. Firstly, it can be used to differentiate LSPs when they are set up. Two LSP attributes, priority attribute (c) and preemption attribute (d), are used for this purpose. A new high priority LSP may preempt a lower priority one if there are not enough resources to support both. The decision is made after the priority attribute of the new LSP is compared with the preemption attribute of the established LSP.

Secondly, prioritisation can be achieved by classifying all traffic flows using a particular LSP into one of eight priority levels as described in (A), and then using

---

[14] This calculation can be done either online by the routers themselves or offline by special servers which periodically send the evaluated routes to the routers [XIAO00].

appropriate queueing and dropping algorithms at output interfaces of LSRs. This approach supports the use of DiffServ over MPLS. In this case, precedence bits within the DSCP (see Fig. 8) can be mapped one-to-one onto the MPLS experimental bits (see Fig. 11).

C. Graceful degradation of hard QoS

A standardised method to modify traffic parameter attributes (a) within and between MPLS domains, without service interruption, is currently being addressed by the IETF [ASH01]. This work, although reasonably matured, has not yet achieved the RFC status.

D. QoS interface with end-user applications

Since MPLS is not designed to directly interface with end-user applications, or even hosts, there is no standardised interface designed for communication between an end-user application and the network.

E. QoS modification

Since MPLS does not interface with end-user applications, there is no standardised direct method to request a QoS modification for a flow using a particular LSP. However, if DiffServ is used over MPLS, and if different classes use LSPs characterised by different traffic attributes, the modification of QoS can be done indirectly by changing the DiffServ class (e.g., through different DSCP marking) of the IP packets transmitted by the application.

F. Traffic Engineering

As already stated, MPLS has been specifically designed to provide traffic engineering. This is achieved through the use of CR-LSPs. MPLS can offer the same basic constraint-based routing infrastructure that ATM employs, without the cell and ATM Adaptation Layer overheads [DYSA00].

G. Scalability

MPLS offers excellent scalability, even better than ATM, due to its ability to stack labels, thus creating arbitrarily nested (aggregated) LSPs.

H. Bandwidth allocation efficiency

MPLS is efficient in assigning bandwidth to flow aggregates traversing LSPs. It is simply not practical to assign a separate label to every flow generated by end-user applications [SEME00].

For average data packets, the overhead due to the use of the additional header is minimal (only 4 bytes). However, if for short packets carrying voice, this overhead represents, the overhead is not negligible. Note that when MPLS uses ATM as the underlying switching technology, MPLS labels can be directly mapped to ATM VPIs/VCIs (see Fig. 5), thus avoiding double label overhead. The overheads related to the distribution of labels and establishment/cancellation of paths are small. They are proportional to the number of LSPs and the frequency of their set up.

Multicasting is not yet standardised for MPLS. However, a well-matured work in this area is currently underway (see [OOMS01] for details).

I. Implementation in commercial networks

It is stressed that MPLS is a relatively new, not yet matured and not well-standardised transmission technology. However, since it offers many valuable transmission features, many vendors, including Cisco [CISC00a] and Nortel [NORT01], already offer rudimentary MPLS in their IP switches[15].

Many carriers are conducting MPLS pilot trials in terrestrial networks. However, companies such as Global One and Concert already offer MPLS-based IP Virtual Private Networks, mainly using Cisco equipment [COMM01].

The use of MPLS over satellite links is a very new research topic. The author is aware of only one research project in this area (see [ROSEN01), with no results available at the time of writing.

J. Implementation in military networks

J.1. ADF perspective

MPLS has not been utilised in Defence networks yet. However, Defence's ISD is currently undertaking trials to evaluate MPLS applicability to carry Backbone Routing Service (BRS) traffic over the DCBN ATM backbone network (see Fig. 3) [CART00].

J.2. US DoD perspective

The US Defense considers the use of MPLS in its strategic DISN network [ROSE99]. It is also being considered for the CINC21 Advanced Concept Technology Demonstrator [ODON00a].

J.3 Coalition perspective

MPLS is being considered for the coalition communication component within the CINC21 ACTD. Trials are planned for financial year 2001 [ODON00a].

[15] Note that both Cisco and Nortel also offer mature proprietary label switching technologies of their own.

3.5 IP Version 6[16]

3.5.1 General Description

IP Version 6 (IPv6), also known as IP Next Generation (Ipng), has been designed to overhaul IPv4 and to allow IP based networks to handle future needs that may arise. The general specification of the protocol is provided in RFC 2460 [DEER98]. Compared with IP v4, the new version offers [STAL00, MILL00]:

- Expanded address space (from 32 bits to 128 bits);
- Simplified header format (some IP version 4 (IPv4) header fields have been dropped or made optional);
- Improved extension headers and options leading to more efficient forwarding;
- Auto-configuration;
- Increased addressing flexibility;
- Additional QoS capability in the form of flow labelling;
- Mandated security and authentication;
- Efficient access to well-known services and mirrored databases by using the concept of anycasting[17].

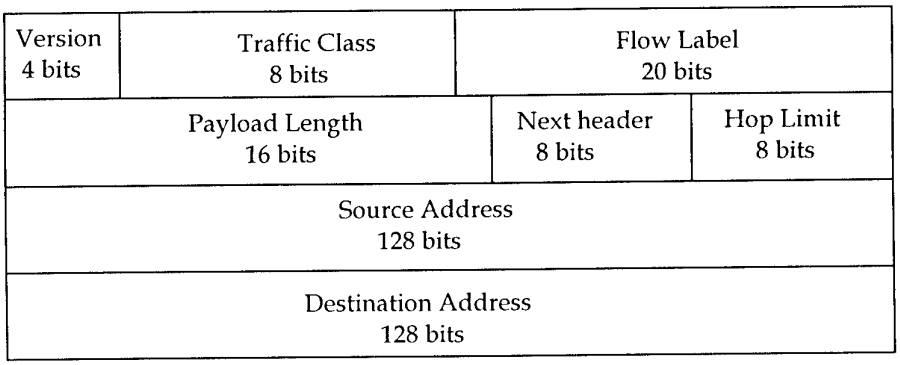


Fig. 12. IPv6 header layout (without extensions).

[16] The author acknowledges the contribution of LT Chris Keogh to this section.

[17] Anycasting is a new service, not yet fully envisioned, in which a packet addressed to a group of nodes, is delivered to only one of them, typically the nearest in the group, according to current routing protocol metrics [BAYN97].

The greatest enhancement to IPv6 is the amount of globally unique addresses that are available. The increased address space removes the need for Network Address Translators (NATs), which are being used to extend the life of IPv4. However, NATs prevent the use of IP-level security between the endpoints of a transaction [KING99].

3.5.2 Assessment of M-QoS Support

A. Commercial QoS

There are two mechanisms supporting QoS in IPv6, namely:

- *Traffic Class marking;*
- *Flow labelling.*

The Traffic Class field (see Fig. 12) replaces the functions that are provided by the Type of Service (TOS) field in IPv4. It allows for differentiation between categories of packet transfer service in the same way as for IPv4. The IP network must be configured to recognise the Traffic Class field otherwise it will be rendered an ineffective function. The DiffServ architecture can utilise this field as presented in Section 3.3.

Flow labelling uses a 20-bit field in the header (see Fig. 12). The RFC 2460 mentioned earlier offers little information on this field. The use of this field is the subject of current research [MILL00]. Theoretically, the field can be used to create labels/tags that the router can use to identify packets in the same flow in order to offer to them soft or hard QoS. But this function is already achieved using MPLS, and it is not clear how both technologies could complement each other.

There is nothing conceptually difficult in using IPv6 in conjunction with IntServ, DiffServ and MPLS presented earlier in this section [ELLI00]. It is expected that IPv6 (even without flow labelling) will offer the same soft and hard QoS characteristics as IPv4.

B. Prioritisation/pre-emption

As with IPv4, prioritisation/preemption of IPv6 packets can be accomplished using DiffServ.

C. Graceful degradation of hard QoS

IPv6 cannot provide this feature alone. This can be achieved through the use of IPv6 in conjunction with DiffServ.

D. QoS interface with end-user applications

As for IPv4, there is no standard QoS interface specified for IPv6 between the end-user application and the network.

E. QoS modification

A QoS modification of a flow can be achieved using IPv6 in conjunction with either DiffServ or IntServ (see Sections 3.2 and 3.3, respectively).

F. Traffic engineering

IPv6 is not designed to provide traffic engineering, but rather relies on any underlying technology to provide this feature. MPLS, presented in the previous section, can be used for this purpose.

G. Scalability

As in the case of IPv4, IPv6 is a datagram technology, which scales very well even for large WANs. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses [DEER98].

H. Bandwidth allocation efficiency

As shown in [ELLI00], if header compression and optional fields are not used, the header penalty strongly depends on the network's traffic mix. For example, IPv6 is much more efficient than IPv4 for large TCP flows (e.g., bulk data transfer using FTP or HTTP). On the other hand, if short UDP packets are used (e.g., with VoIP), IPv6 creates a significantly larger overhead compared to IPv4. Note that header compression in IPv6 packets can be achieved using an algorithm proposed in [DEGE99].

IPv6 offers similar multicast capabilities as IPv4.

I. Implementation in commercial networks

Whilst IPv6 has addressed many of the problems associated with IPv4, it has indirectly acted as a catalyst for the development of key capabilities to be introduced to IPv4 [GROS00]. Although the long-term need for the IPv6 introduction is obvious, there is currently little market demand for it. One reason is a very limited number of standard applications prepared for this version. Another reason is the need to provide either translation between IPv4 and IPv6 protocol stacks or some form of tunnelling when IPv6 "islands" are added to IPv4 legacy networks. As for the former, many routers are

being manufactured and shipped with a dual IPv4/IPv6 stack to ease the transition process.

As for the tunnelling, it is used, for example, by the 6Bone initiative [IPV601]. Obviously, tunnelling increases overheads.

The author is not aware of any IPv6 trials over GEO satellite links.

J. Implementation in military networks

J.1. ADF perspective

Currently, there are no plans to implement or even trial IPv6 in Defence networks. Its use will likely be considered only when the commercial world and/or coalition partners start using the new version on a large scale.

J.2. US DoD perspective

There are no immediate plans to use IPv6 in US DoD networks. However, Mitre Co., supporting the US DoD, plans to undertake limited trials of this technology in the near future [ODON00].

J.3 Coalition perspective

IPv6 is being considered for coalition communications within the CINC21 ACTD. Trials are planned for FY 2001 [ODON00a].

4. Proposed Solution

The assessment presented in Section 3 clearly shows that there is no single technology capable of providing all the M-QoS features. Instead, we propose to use a combination of the analysed technologies, as shown in Fig. 13.

The proposed combination includes:

a. IPv4/IPv6

These protocols 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 (see discussion in Section 3.3.2). DSTO is currently investigating this problem [BLAI01]. If the results are negative, ATM may be used instead.

Note that the inclusion of IPv6 is due to the expected gradual replacement of IPv4 by the newer version, rather then its specific QoS features.

b. DiffServ

This technology will provide both hard and soft QoS as well as graceful degradation in hard QoS to IP flows. Both the fixed and tactical trunk networks of the Defence communications infrastructure will be divided into DiffServ domains as shown in Fig. 13. DiffServ will be augmented by the use of bandwidth brokerage.

Bandwidth Brokers (BBs), apart from the typical functions described in Section 3.3.1), will also undertake all military specific functions related to the provision of M-QoS in the Defence Core, including:

- Communication with end-user applications using the concept of M-QoS interface described in [BLAC00a] and briefly presented in Section 1. It is noted that MIN Branch within DSTO is currently finishing the design of software for a standardised IP-based M-QoS interface between end-user applications and BBs. Note that the interface will also enable an application to request QoS modifications;
- Authentication of military users;

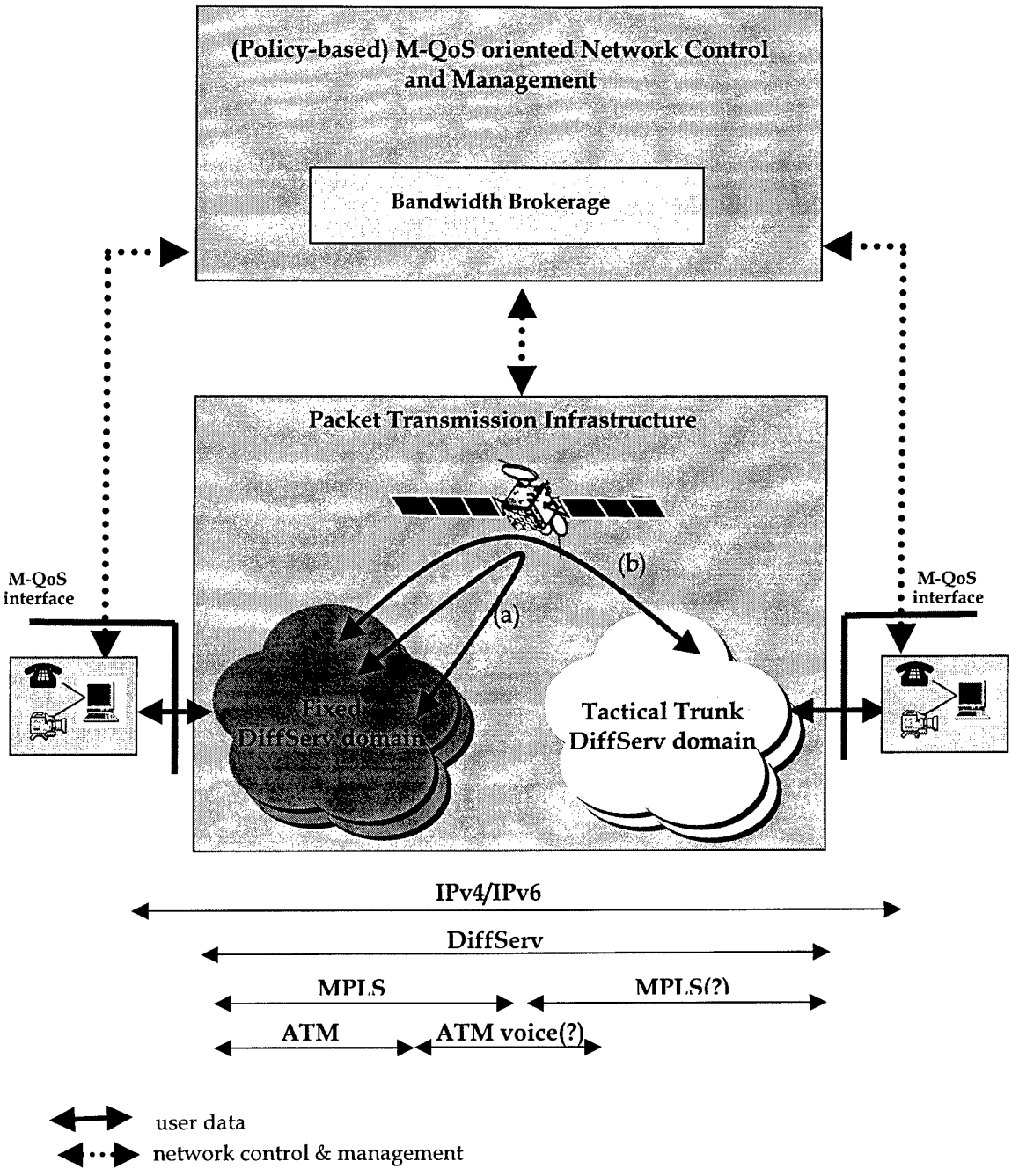


Fig. 13. The proposed combination of transmission technologies and supporting them network control and management. ((a,b) – see text.)

- Evaluation of the Ultimate Priority of military flows according to their military value;
- Ordering, if necessary, the ingress routers to preempt some flows/flow aggregates in order to admit new flows of higher priority.

Following the arguments presented in [BLAC00a], it is proposed to use Policy-based Network Management (PBNM) to support the implementation of DiffServ and bandwidth brokerage as presented in Fig. 13. It is noted that the IETF has developed a PBNM framework to support IP networks in general [MOOR01a, SNIR01], and DiffServ in particular [MOOR01b]. The relationship between bandwidth brokage and PBNM has not been addressed yet by the IETF. It is noted that the Internet2 initiative identifies this as an area of future research.

c. *MPLS*

MPLS will be used to provide traffic engineering, mainly in the terrestrial part of the Core and possibly over a satellite (depicted as (a) in Fig. 13) to provide back-up links to the terrestrial Core, thus increasing its survivability. MPLS may also be used between the fixed and tactical trunk domains (depicted by (b) in Fig. 13). The need for this requires further study.

d. *ATM*

ATM will still be used in the terrestrial part of the Defence Core Backbone Network, firstly to support MPLS switching and secondly to continue carrying voice traffic until VoIP is implemented on a large scale. It is anticipated that the protocol stack composed of IP over MPLS over ATM will gradually be replaced by IP over Sonet/SDH or even directly IP over fibre. These new technologies will be supported by the Generalised Multi-Protocol Label Switching (GMPLS)[18] [ASHW01] instead of MPLS.

As indicated in (a), ATM may be required to transport voice over slow satellite links if IPv4/IPv6 and DiffServ do not satisfy the low jitter requirements.

The proposed combination of technologies is very well scalable and bandwidth efficient due to the use of DiffServ and MPLS. There are also strong indications that the commercial world, the US DoD and coalition initiatives will embrace such a combination of technologies, at least to provide commercial-type QoS.

As to a coalition environment, it is noted that the concept of M-QoS and the proposed above combination of technologies to support M-QoS have been accepted for a detailed investigation within the Project Arrangement (PA) on Coalition Network Management. The PA, which is sponsored by The Technical Cooperation Program (TTCP), was signed in October 2000 by Australia, the US and Canada. It is aimed at designing and exploring effective network management mechanisms in a coalition environment.

[18] GMPLS is a development of MPLS currently being investigated by the IETF.

A number of issues need to be resolved and clarified before the proposed combination of technologies can be treated as a complete solution for the Defence Core. These include:

- Design of a viable set(s) of DiffServ classes of Defence traffic;
- Performance (e.g., delay, bandwidth) implications of BB-to-BB communication over a satellite link;
- Mapping between DiffServ classes and MPLS paths, and between the latter ones and ATM VCs/VPs;
- Use of MPLS for satellite communication between fixed and tactical trunk domains;
- Relationship between Bandwidth Brokers and the PBNM in the Defence context, and performance implications of using the PBNM to manage both fixed and tactical trunk DiffServ domains connected by a satellite link;
- Impact of the proposed combination of technologies on the currently used/planned security architectures in the Defence Core.

5. Conclusion and Recommendation

The major findings of this report can be summarised as follows:

a. The report shows that none of the analysed transmission technologies supporting commercial QoS can completely fulfil the criteria considered in this report as vital to implement Military oriented QoS (M-QoS) in the Defence terrestrial/satellite Core;

b. The report proposes to use IPv4/IPv6, DiffServ, MPLS and ATM as building blocks for the future M-QoS capable Defence Core. Both fixed and tactical trunk Defence networks will be divided into DiffServ domains, each equipped with a bandwidth broker responsible for the proper provision of bandwidth within its domain, and between its domain and peer domains;

c. Bandwidth brokers (BBs) are the network entities which will undertake all military specific functions related to the provision of M-QoS in the Defence Core;

d. The report identifies Policy-based Network Management (PBNM) as an important mechanism to facilitate the implementation of M-QoS in a flexible way;

e. For the proposed combination of technologies, a number of issues require further study, among which the most challenging are:

   - Bandwidth implications for BB-to-BB communication over a satellite link;
   - Relationship between Bandwidth Brokers and PBNM in the Defence context, and performance implications of using PBNM to manage fixed and tactical trunk DiffServ domains connected by a satellite link;
   - Impact of the proposed combination of technologies on the currently used/planned security architecture(s) for the Defence Core.

Based on the report's findings, the following is recommended:

A. Prepare a concept of network transmission, control and management architecture that would offer M-QoS features over the Defence terrestrial/satellite Core communications infrastructure;

B. Undertake a detailed study on how PBNM could be implemented in an efficient and reliable way in the Defence terrestrial/satellite Core environment;

C. Analyse the impact of the Defence Core security architecture on the proposed transmission infrastructure.

6. References

[ADVA00] A. Schmidt, K. Kalichin (Advantra), "Joint Project 2047 Phase 1A DWACN", DSDN Workshop, Mt Macedon, Vic., 12-13 Sept., 2000.

[AKIL97] I. Akildiz, S. Jeong, "Satellite ATM networks", IEEE Communications Magazine, July 1997.

[ARIN99] P. Arindam, "QoS in Data Networks: Protocols and Standards", Ohio State University, Nov. 1999.

http://www.cis.ohio-state.edu/~jain/cis788-99/qos_protocols/index.html

[ARMI00] G. Armitrage, "MPLS: The Magic Behind the Myths", IEEE Communications Magazine, January 2000.

[ASH01] J. Ash et al, "LSP Modification Using CR-LDP", IETF Draft draft-ietf-mpls-crlsp-modify-03.txt, Feb. 2000.

[ASHW01] P. Ashwood-Smith et al, "Generalized MPLS - Signaling Functional Description", IETF draft-ietf-mpls-generalized-signaling-04.txt, May 2001.

[ATMFM96] ATM Forum, "ATM Forum traffic Management Specification- Version 4.0", April 1996.

[ATMFS96] ATM Forum, "ATM User-Network Interface (UNI) Signalling Specification Version 4.0", July 1996.

[ATM0148] ATM Forum, "Modification of Traffic Descriptor for an Active Connection, Addendum to UNI 4.0, PNNI 1.0, and AINI", July 2000.

[AWDU99] D. Awduche et al., "Extension to RSVP for Traffic Engineering" IETF, draft draft-ietf-mpls-rsvp-lcp-tunnel-04.txt, Sept. 1999.

[AWDU99b] D. Awduche et al., "Requirements for Traffic Engineering Over MPLS" IETF RFC 2702, Sept. 1999.

[ADYS99] G. Apostolopoulos et al., "Intradomain QoS Routing in IP Networks: Feasibility and Cost/Benefit Analysis", IEEE Communications Magazine, Sept./Oct. 1999.

[BAKE00] F. Naker, et al, " Aggregation of RSVP for Ipv4 and Ipv6 reservations", IETF Draft: draft-ietf-issll-rsvp-aggr-02.txt, March 2000.

[BAYN97] "IPv6", Bay Networks, White Paper, 1997.

[BERN00] J. Bernet et al., "A Framework for Integrated Services Operation over DiffServ Networks", IETF Draft: draft-ietf-issll-diffserv-rsvp-05.txt, May 2000.

[BERN00a] Y. Bernet, "The Complementary Roles of RSVP and Differentiated Services in Full-Service QoS Network", IEEE Communications Magazine, Feb. 2000.

[BLAC00a] P. Blackmore, P. George, M. Kwiatkowski "A Quality of Service Interface for Military Applications", proceedings MILCOM 2000 conference, Los Angeles, Oct 2000.

http://www-cd/projects/core_comms/documents/papers/management/milcom00_final.doc

[BLAC00b] P. Blackmore, P. George, M. Kwiatkowski, C. Tran, T. Tyszta, "A Quality of Service Interface to Support Next Generation Military Applications", DSTO Technical Report, Nov. 2000.

[BLAC01] P. Blackmore, P. George, K. Hui, P. Kerr, M. Kwiatkowski, K. Northeast, M. Rossiter, R. Taylor, C. Tran, "Review of the Defence Core Communications Environment", DSTO General Document, DSTO-GD-0275, Feb. 2001.

[BLAI01] Bill Blair, DSTO, *personal communication*, June 2001.

[BLAK98] S. Blake et al, "An Architecture for Differentiated Services", IETF RFC 2475, Dec. 1998.

[BOWM98] L. Bowman, R. Riehl, S. Shad, "Defence Information System Network (DISN) Asynchronous Transfer Mode (ATM) Goal Architecture and Transition Strategy", MILCOM'98, Boston, USA, 1998.

[BRAD97] R. Braden et al. "Resource reSerVation Protocol - Versio 1 Functional Specification", IETF RFC 2205, Sept. 1997.

[CANS99] D. H. Cansever, M. Klun, " Differentiated Services to Scale Internet Access", SPIE Conference on Internet II: Quality of Service and Future Directions, Boston, USA, Sept. 1999.

[CALL99] R. Callon et al, " A Framework for Multiprotocol Label Switching", IETF Draft draft-ietf-mpls-framework-05.txt, Sept 1999.]

[CART00] S. Carter (DISG), "MPLS Strategy", DSDN Workshop, Mt Macedon, Australia, 12-13 Sept., 2000.

[CASN99] S. Casner, V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", RFC 2508, Feb. 1999.

[CFBL00] QoS Experiment Group CFBLNet, "QoS Tests in Preparation of JWID 2001 on CFBLNet", slide presentation, Nov. 2000.

[CHEN95] T. Chen, "ATM Switching Systems", Artech House, 1995.

[CHIU99] A. Chiu, "Current Status of Quality of Service in IP", SPIE Conference on Internet II: Quality of Service and Future Directions, Boston, USA, Sept. 1999.

[CHIT00] P. Chitre, "ATM and Internet via Satellite", Proceedings MILCOM 2000 Conference, Los Angeles, Oct 2000.

[CISC00] "Congestion Management Overview", Cisco Documentation, Aug. 2000.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt2/qcdconghtm#xtocid84007

[CISC00a] "Cisco IOS Software and Multiprotocol Label Switching", Cisco, 2000.

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/iosmp_ai.pdf

[CUEV99] E. Cuevas, "The Development of Performance and Availability Standards for Satellite ATM Networks", IEEE Communications Magazine, July 1999.

[DEER98] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6), Specification", IETF RFC 2460, Dec. 1998.

[DEGE99] M. Degermark, B. Nordgren, S. Pink, "Header Compression for IPv6", RFC 2507, Feb. 1999.

[DIBE99] R. DiBella, DISC, "The Defence Organisation's Information Infrastructure", presentation, July 1999.

[DYSA00] D. McDysan, " QoS & Traffic Management in IP & ATM Networks", McGraw Hill, 2000.

[DMO00] Telstra, "Data Mode of Operation (DMO)", presentation, Canberra, Oct 2000.

http://web-cd/Projects/core_comms/documents/presentations/general/fed_gov_ACT_dmo.ppt

[EICH00] G. Eichler et al, "Implementing Integrated and Differentiated Services for the Internet with ATM Networks: A Practical Approach", IEEE Communications Magazine, January 2000.

[ELLIO00] B. Elliott et al, "IPv6 Currnet Technology Status and its Impact on the Army's Tactical Internet", BBN Technologies, Febr. 2000.

[ELMO98] F. EL-Mokadem, "Evaluation of Network Performance Objectives over DISN ATM Connections", MILCOM'98, USA, 1998.

[FARS00] J. Farserotu, R. Prasad, "A Survey of Future Broadband Multimedia satellite Systems, Issues and Trends", IEEE Communications Magazine, June 2000.

[GEOR01] P. George, et al, "Implementation of the standardised Military oriented Quality of Service Interface for IP-oriented Networks", DSTO Technical Report, *in preparation*, May 2001.

[GHAN99] A. Ghan, "Traffic Engineering Standards in IP Networks Using MPLS", IEEE Communications Magazine, Dec. 1999.

[GROS00] Grossetete, P., M, McNealis.. "Cisco Systems Statement Of Direction IP Version 6", 2000

http://www.cisco.com/warp/public/732/ipv6/index.html

[HADJ98] S. Hadjipanteli, P. Kumar, S. Wang, "Defense Information system Network (DISN)/NIPRINET Modelling and Analysis for Unclassified ATM Network", MILCOM'98, USA, 1998.

[HEIN99] J. Heinanen et al, "Assured Forwarding PHB Group", IETF RFC 2597, June 1999.

[HERZ00a] S. Herzog, "RSVP Extensions for Policy Control", IETF RFC 2750, Standards Track, Jan. 2000.

[HERZ00b] S. Herzog, "Signalled Preemption Priority Policy Element", IETF RFC 2751, Standards Track, Jan. 2000.

[HUST00] G. Huston, "Next Steps for the IP QoS Architecture", IETF Draft draft-iab-qos-00.txt, March 2000.

[HUNT01] B. Hunter, DISG, *personal communication*, May 2001.

[INT201] Internet2, http://www.internet2.edu/

[IPHY01] IPHighway Co., 2001, http://www.iphighway.com/

[IPV601] The 6Bone Initiative, 2001, http://www.6bone.net/

[IUOR99] A. Iuoras et al, " Quality of Service-oriented protocols for resource management in packet-switched satellites", International Journal of Satellite Communications, Vol. 17, 1999.

[JACO90] V. Jacobson, "TCP/IP Compression for Low-Speed Serial Links", RFC 1144, IETF, Feb. 1990.

[JACO99] V. Jacobson et al, "An Expedited Forwarding PHB", IETF RFC 2958, June 1999.

[KING99] King, S. et al. 1999. "The case for IPv6", available from: http://www.6bone.net/misc/case-for-ipv6.html]

[KING00] J. Kingston, "Dynamic Precedence fro Military IP Networks", proceedings MILCOM 2000 conference, Los Angeles, Oct 2000.

[KWIA99a] M. Kwiatkowski, P. George, "A Network Control and Management Framework Supporting Military Quality of Service", MILCOM'99, Atlantic City, USA, October 1999.

http://web-cd/projects/core_comms/documents/papers/management/milcom99_publ.doc

[KWIA99b] M. Kwiatkowski, "Network Control and Management Architectural Framework Supporting Military Quality of Service", DSTO Technical Report, DSTO-TR-0871, Sept. 1999. http://203.10.217.101/corporate/reports/DSTO-TR-0871.pdf

[LEPP00] Jerry Leppert, AFRL/IFGA, *Personal Communication*, March 2000.

[LUCE00] Proceedings of the PSAX 1250 Access Concentrator Training Course, Lucent Technologies, Oct. 2000.

[MILL00] M. Miller, "*Implementing IPv6*", M&T Books, USA, 2000.

[MIRH00] M. Mirhakkak, et al, "A New Approach for Providing Quality-of-Service in a Dynamic Network Environment", proceedings MILCOM 2000 conference, Los Angeles, Oct. 2000.

[MOOR01a] B. Moore et al, "Policy Core Information Model -- Version 1 Specification", RFC 3060, IETF, Feb. 2001.

[MOOR01b] B. Moore et al, "Information Model for Describing Network Device QoS Datapath Mechanisms", draft-ietf-policy-qos-device-info-model-03.txt, IETF, May 2001.

[M60] "Recommendation M.60 - Maintenance Terminology and Definitions", ITU-T, March 1993.

[NICH98] K. Nichols et al, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF RFC 2474, Dec. 1998.

[NORT01] "MPLS", Nortel Networks, 2001.
http://www.nortelnetworks.com/corporate/technology/mpls/index.html

[ODON00] Ch. O'Donnell, The Mitre Co., *personal communication*, October, 2000.

[ODON00a] Ch. O'Donnell,"CINC 21 - Thrust III", AITS-JPO presentation, May 2000.

[OOMS01] D. Ooms, et al, "Framework for IP Multicast in MPLS", IETF Internet Draft draft-ietf-mpls-multicast-05.txt, Jan. 2001.

[PETR99] M. Petrovsky, "Policy capabilities Help Drive RSVP's Renaissance", NWFUSION, May 1999.
http://www.nwfusion.com/archive/1999b/0705petrovsky.html

[PNNI96] ATM Forum, "Private Network-Network Interface Specification - version 1.0", March 1996.

[ROSE99] J. Rose, DISA-ITESO, *personal communication*, Oct. 1999.

[ROSE01] E. Rosen, "Multiprotocol Label Switching Architecture", IETF RFC 3031, Jan. 2001.

[ROSEN01] C. Rosenberg, T. Ors, "Multi Protocol Label Switching over Satellite", Research Project, Purdue University, USA, 2001.
http://dynamo.ecn.purdue.edu/~cath/projectMPLSsat.htm

[RUBE01] R. Rubenstein, "Operators feeling more secure about MPLS", Communications Week International, 5 March 2001.

[QBONE] Qbone home web page, http://qbone.internet2.edu/

[QBONEa] QBone Bandwidth Broker Architecture (Work in Progress), June 2000.
http://qbone.internet2.edu/bb/bboutline2.html

[QOSF99] QoS Forum, "The Need for QoS", White Paper, July 1999.
http://www.qosforum.com/tech_resources.htm

[Q.2931] ITU-T Recommendation Q.2931, "B-ISDN DSS2 User-Network Interface (UNI) Layer 3 Specification for Basic Call/Connection Control", 1995.

[Q.2971] ITU-T Recommendation Q.2971, "B-ISDN DSS2 UNI Layer 3 Specification for Point-to-Multipoint Call/Connection Control", 1995.

[Q.2963.1] ITU-T Recommendation Q.2963.1, "Digital Subscriber Signalling System No. 2 - Connection modification: Peak cell rate modification by the connection owner", 1999.

[Q.2963.2] ITU-T Recommendation Q.2963.2, "Digital Subscriber Signalling System No. 2 - Connection modification: Modification procedures for sustainable cell rate parameters", 1997.

[Q.2963.3] ITU-T Recommendation Q.2963.3, Digital Subscriber Signalling System No. 2 - Connection modification: ATM traffic descriptor modification with negotiation by the connection owner", 1998.

[SANT01] R. Santitoro, O. Slupecki, "IP Differentiated Services on Passport 6K/7K/15K", Nortel Networks, 2001.

[SEME00] Ch. Semeria, " Multiprotocol Label switching - Enhancing Routing in the New Public Network", White Paper, Juniper Networks, 2000.

[S142099] ITU-R, "Performance for broadband integrated services digital network asynchronous transfer mode via satellite", Nov. 1999.

[S142400] ITU-R, "Availability objectives for a hypothetical reference digital path when used for the transmission of B-ISDN asynchronous transfer mode in the fixed-satellite service by geostationary orbit satellite systems using frequencies below 15 GHz", Jan. 2000.

[SHEN97] S. Shenker, C Partrige, R. Guerin, "Specification of Guaranteed Quality of Service", IETF RFC 2212, Sept. 1997.

[SHEN97a] S. Shenker, J. Wroclawski, "Network Element Service Specification Template", IETF, RFC 2216, Sept. 1997.

[SHVO98] W. Shvodian, "Multiple Priority Distributed Round Robin MAC Protocol for Satellite ATM", MILCOM'98, Boston, USA, 1998.

[SNIR01] Snir Y, Ramberg Y, Strassner J, Cohen R, "Policy Framework QoS Information Model", draft-ietf-policy-qos-info-model-03.txt, April 2001.

[SNIR00b] Snir Y, Ramberg Y, Strassner J, Cohen R, "QoS Policy Model", draft-ietf-policy-qos-schema-00.txt, Febr. 2000.

[STAL00] W. Stallings, "Data and Computer Communications", Prentice-Hall, New Jersey, 2000.

[STAR99] QoS Forum, "QoS protocols & architectures - White paper", July 1999.
http://www.qosforum.com/white-papers/qosprot_v3.pdf

[STEL99] R. Stelzl, "The Siemens Bandwidth Broker", Proceedings of the First Joint Internet2 / DOE QoS Workshop "QBone: Early Experiences and the Road Ahead", Houston, USA, Feb. 2000.

http://www.internet2.edu/qos/houston2000/proceedings/Stelzl/20000209-QoS2000-Stelzl.pdf

[STIM01] Phil Stimson, DSTO, *personal communication,* June 2001.

[SWAL99] G. Swallow, "MPLS Advantages for Traffic Engineering", IEEE Communications Magazine, Dec. 1999.

[TANE96] A. Tanenbaum, "Computer Networks", International Third Edition, Prentice Hall, New Jersey, 1996.

[TEIT99] B. Teitelbaum *et al,* "Internet2 Qbone: Building a Testbed for Differentiated Services", IEEE Communications Magazine, Sept./Oct. 1999.

[VAKI98] F. Vakil, "A Heuristic for Interoperability Assurance in ATM networks", MILCOM'98, USA, 1998.

[WHIT97] P. White, "RSVP and Integrated Services in the Internet: A Tutorial", IEEE Communications Magazine, May 1997.

[WILK01] Darren Wilksch, DSTO, *personal communication,* April 2001.

[WROC97a] J. Wroclawski, "The Use of RSVP with IETF Integrated Services", IETF RFC 2210, Sept. 1997.

[WROC97b] J. Wroclawski, "Specification of the Controlled-Load Network Element Services", IETF RFC 2211, Sept. 1997.

[WROC01] J. Wroclawski, A. Charny, "Integrated Service Mappings for Differentiated Services Networks", IETF, draft-ietf-issll-ds-map-01.txt, Febr. 2001.

[YAVA00] R. Yavatkar et al, "A Framework for Policy-based Admission Control", IETF RFC 2753, Jan. 2000.

[XIAO99] X. Xiao, L. Ni, "Internet QoS: A Big Picture", IEEE Communications Magazine, March/April 1999.

[XIAO00] X. Xiao, "Traffic Engineering with MPLS in the Internet", IEEE Communications Magazine, March/April 2000.

DISTRIBUTION LIST

Report title
Preliminary Assessment of Transmission Technologies to Support Military Oriented QoS

Author
Marek Kwiatkowski

AUSTRALIA

DEFENCE ORGANISATION

Task sponsor

Director General Command, Control, Communications and Computers (DGC4)
Mr. Claude D'Abrera (DDFC), R1-3-A079A
CMDR Paddy Torrens (DD-MOBILE COMMUNICATIONS), R1-3-A067
WGCDR Eric Gidley (DDLRC), R1-3-A103

S&T Program

Chief Defence Scientist
FAS Science Policy
AS Science Corporate Management
Director General Science Policy Development
} shared copy

Counsellor Defence Science, London (Doc Data Sheet only)
Counsellor Defence Science, Washington (Doc Data Sheet only)
Scientific Advisor to MRDC Thailand (Doc Data Sheet only)
Scientific Advisor Joint
Navy Scientific Adviser (Doc Data Sheet and distribution list only)
Scientific Adviser - Army (Doc Data Sheet and distribution list only)
Air Force Scientific Adviser
Director Trials

Aeronautical and Maritime Research Laboratory
Director

Electronics and Surveillance Research Laboratory
Director (Doc Data Sheet and distribution list only)

Chief of Communications Division
Research Leader Military Information Networks
Head Network Architectures
Head Wireless Systems
Head Network Management
Head Distributed Systems Group (Fern Hill)

Marek Kwiatkowski (DSTO/CD/MIN)

DSTO Library and Archives
Library Fishermens Bend (Doc Data sheet only)
Library Maribyrnong (Doc Data sheet only)
Library Salisbury (1 copy)
Australian Archives
Library, MOD, Pyrmont (Doc Data sheet only)

US Defense Technical Information Center, 2 copies
UK Defence Research Information Centre, 2 copies
Canada Defence Scientific Information Service, 1 copy
NZ Defence Information Centre, 1copy
National Library of Australia, 1 copy

Capability Development Division
Director General Maritime Development (Doc Data Sheet only)
Director General Land Development (Doc Data Sheet only)
Director General Aerospace Development (Doc Data Sheet only)

Defence Materiel Organisation
DCNSPO, R3 Russell Offices, Canberra

Knowledge Staff
Director General Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (DGISREW) R1-3-A142, Canberra, ACT 2600
Director General Defence Knowledge Improvement Team (DGDKNIT) R1-3-A141, Canberra, ACT 2600 (Doc Data Sheet only)

Navy
SO (Science), Director of Naval Warfare, Maritime Headquarters Annex, Garden Island, NSW 2000 (Doc Data Sheet only)
Directorate of Navy Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare, CP4-4-043

Army
ABCA Standardisation Officer, Puckapunyal (4 copies)
SO (Science), DJFHQ(L), MILPO Enoggera, Queensland 4051 (Doc Data Sheet only)
NAPOC QWG Engineer NBCD c/-DENGRS-A, HQ Engineer Centre Liverpool Military Area, NSW 2174 (Doc Data Sheet only)

Intelligence Program
DGSTA Defence Intelligence Organisation
Head, Information Centre Defence Intelligence Organisation

Information Systems Division
HISD, CP1-5-001, Department of Defence, Canberra ACT 2600
DGIS-ISD, DKN-N1-007
DDC-ISD, DKN-N1-005
Mr. Ric Glenister, DKN-N1-30
Mr. Bert Hunter, DKN-N2-A11-A13

Corporate Support Program
Library Manager, DLS Canberra

Universities and Colleges
Australian Defence Force Academy
Library
Serials Sections (M list), Deakin University Library, Geelong, 3217
Senior Librarian, Hargrave Library, Monash University (Doc Data Sheet only)
Librarian, Flinders University

Other Organisations
NASA (Canberra)
AusInfo
State Library of South Australia

OUTSIDE AUSTRALIA

Abstracting and Information Organisations
Engineering Societies Library, US
Documents Librarian, The Center for Research Libraries, US

Information Exchange Agreement Partners
Acquisitions Unit, Science Reference and Information Service, UK
Library - Exchange Desk, National Institute of Standards and Technology, US

SPARES (5 copies)

Total number of copies: 56

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Preliminary Assessment of Transmission Technologies to Support Military Oriented QoS

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Marek Kwiatkowski

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Edinburgh SA 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1207	AR-012-014	Technical Report	September 2001

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
E 8709-7-16	99/150	C4	55	113

13. URL
http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1207.pdf

14. RELEASE AUTHORITY

Chief, Communications Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE CENTRE, DIS NETWORK OFFICE, DEPT OF DEFENCE, CAMPBELL PARK OFFICES, CANBERRA ACT 2600

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT Yes

18. DEFTEST DESCRIPTORS

Network Control, Network Management, Computer Architecture, Switching Systems, Quality of Service, Military Networks

19. ABSTRACT

This report is aimed at assessing some promising available or emerging commercial transmission technologies regarding their potential support of Military oriented Quality of Service (M-QoS) in the terrestrial/satellite Defence Core communications infrastructure. The chosen technologies are ATM, IP Integrated Services, IP Differentiated Services, MPLS and IPv6. The criteria of interest include the support of commercial QoS, prioritisation/preemption, graceful degradation of QoS, QoS interface with end-user applications, QoS modification, traffic engineering, scalability, bandwidth usage efficiency, and implementation in commercial as well as military networks. The report shows that none of the considered technologies can support all the criteria in isolation. However, a combination of IPv4/IPv6, Differentiated Services (augmented by bandwidth brokerage), MPLS and in some cases ATM is proposed in the report as a good candidate to build the future M-QoS capable Defence Core. More research is required to fully assess the applicability of the proposed combination to achieve M-QoS.

TECHNICAL REPORT DSTO-TR-1207 AR-012-014 SEPTEMBER 2001

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

ELECTRONICS AND SURVEILLANCE RESEARCH LABORATORY
PO BOX 1500 EDINBURGH SOUTH AUSTRALIA, 5111
AUSTRALIA, TELEPHONE (08) 8259 5555