



ATIS-0100003

User Plane Priority Levels for IP Networks and Services

TECHNICAL REPORT



The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< <http://www.atis.org/> >

ATIS-0100003, *User Plane Priority Levels for IP Networks and Services*

Is an ATIS Standard developed by the **Network Reliability and Security Working Group** under the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2006 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org/> >.

Printed in the United States of America.

Technical Report on

User Plane Priority Levels for IP Networks and Services

Secretariat

Alliance for Telecommunications Industry Solutions

Approved November 2004

Abstract

This Technical Report (TR) was developed as a formal response to a request from the ATIS sub-committee PTSC-SAC for guidance on user plane priority levels in IP networks. This TR proposes three levels of connection admission control priority for the user plane communications traffic in IP networks. It also proposes that all emergency communications (*e.g.*, ETS and E911) be given the highest priority for call/session setup.

FOREWORD

This Technical Report (TR) provides a formal response to a request from ATIS sub-committee PTSC-SAC (formerly T1S1.7) for guidance on the number of user plane priority levels in IP networks.

This TR is intended for providers of IP-based communications networks and services, communications equipment suppliers, and government agencies responsible for addressing emergency situations.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) – formerly T1A1 – develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PRQC Secretariat, 1200 G Street N.W., Suite 500, Washington, DC 20005.

The Network Reliability and Security Working Group on Network Performance, Reliability, and Quality of Service was responsible for the development of this document, and had the following officers and participants:

- O. Avellaneda, Chair
- S. Makris, Vice Chair
- F. Kaudel, Chief Editor
- P. Tarapore, A. Nguyen, and A. Webster; Technical Editors
- C. Underkoffler, ATIS Chief Editor

Active Participants:

J. Ash	P. Kimbrough	S. Sayers
O. Avellaneda	J. Lankford	N. Seitz
C. Bailey	S. Makris	P. Tarapore
J. Bennett	A. McCain	A. Webster
M. Dolly	A. Nguyen	R. Wohlert
C. Dvorak	R. Paterson	

TABLE OF CONTENTS

FOREWORD	II
TABLE OF CONTENTS	III
1 PURPOSE	1
2 SCOPE	1
3 APPLICATION	2
4 RELATED WORK	3
5 CAC PRIORITY PRINCIPLES	3
6 RECOMMENDATION FOR CAC PRIORITY LEVELS	4
7 FLEXIBILITY	5
8 CONCLUSION	5
9 DEFINITIONS	5
10 ABBREVIATIONS AND ACRONYMS	6
11 REFERENCES	6

Technical Report on

User Plane Priority Levels for IP Networks and Services

1 PURPOSE

The ATIS sub-committee PTSC-SAC (formerly T1S1.7) submitted a formal request to the ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC) ^[1] – formerly known as T1A1 – for guidance on the number of priority levels for IP services. The basis for this request stems from a need to develop priority-based signaling extensions in appropriate protocols (*e.g.*, Session Initiation Protocol – SIP) such that critical services such as Emergency Telecommunications Services (ETS) ^[2] and E911 are preferentially recognized for call/session setup in IP networks.

This document is the formal response from PRQC to the PTSC-SAC. It recommends three priority class levels for IP services in the user plane. It also recommends that the highest priority level be reserved for emergency services such as ETS and E911.

2 SCOPE

From the perspective of the network, it is expected that future IP networks will be truly “converged.” That is, all forms of communications traffic will be handled by such networks – control plane traffic (*e.g.*, routing and signaling messages), emergency services, real-time voice and video services, data services, Virtual Private Network (VPN) services, as well as traditional “Best Effort” traffic. In such an environment, it is important to assign priority classifications and establish rules for capacity reservation and admission such that critical services (*e.g.*, control plane traffic and emergency services) are recognized and accepted for call/session setup and completion (or simply carried in the case of non-session oriented traffic) over other services in case of network overloads or failures. As service flows can be expected to traverse multiple network domains, priority classification is an important step in the development of the necessary signaling protocol extensions as well as the mechanisms for enabling preferential treatment of critical services.

The scope of this recommendation is limited to the determination of user (or media/bearer) plane priority class levels for communications over IP networks. The underlying support for this recommendation is based on the potential impact on IP services due to failure or congestion conditions. Specifically, the recommendation seeks to cast a broad view on priority classification, namely; what should the proper number of classes be such that critical services are given the highest probability of successful call/session setup and completion under congested conditions. For example, it is recognized that a class of “emergency services” can comprise Federal ETS as well as local E911 calls and that this class of traffic requires priority treatment in case of emergency. The goal of this document is to distinguish this class of traffic from other less critical classes of traffic. However, this document does not seek to “fine tune” the treatment of different traffic types within a broad priority class or level. Thus, the ability to distinguish between service types within any given priority class (*e.g.*, distinguish between ETS and E911 services in the emergency service class) is beyond the scope of this document.

As stated above, it is recognized that control plane traffic is critical for ensuring smooth network operations as well as inter-domain signaling interactions. However, control plane traffic priority determination and its relative criticality compared to user plane traffic (*e.g.*, highest available priority for control plane traffic over all user plane traffic) is not considered at this stage for the following reasons:

- ◆ *The initial request from the Protocol Inter-working Committee was driven by a need to understand the priority levels available/supported by the user plane traffic. Call control messages in protocols such as SIP can then be mapped to the recommended priority levels. These levels can also assist in follow-on questions such as mapping the recommended priority levels to priorities within the packet queuing algorithm at the network border element to the IP backbone [3].*
- ◆ *The composition of control plane traffic can vary depending on the type of IP networking capabilities ranging from simple Best Effort services only to more sophisticated MPLS-based services such as VPNs. Thus intra-domain control plane traffic can comprise, for example, OSPF messages, as well as protocol messages in support of Multi-Protocol Label Switching (MPLS) features. In addition, control plane traffic can also include inter-domain messages representing BGP and signaling protocol messages (*e.g.*, SIP messages). The exact mix and volume of intra and inter-domain control plane traffic as a proportion of total network traffic is somewhat uncertain and a matter for further study.*
- ◆ *The question of the relative importance of the various forms of control plane traffic compared to customer-based bearer plane traffic has yet to be addressed. For example, it may be essential to reach agreements on the relative priority of inter-domain control plane traffic. However, service carriers may chose to treat intra-domain control plane traffic according to their individual network needs.*

Control plane traffic priority questions are very important and they need to be addressed in future efforts. It is hoped that addressing user plane traffic priority questions as a first step, can eventually lead towards acceptable agreements on control plane traffic questions.

3 APPLICATION

The priority level classification is based on the following premise: under reduced bandwidth conditions, the critical issue for an IP network is the ability to recognize and admit higher priority traffic flows into the network. This can be referred to as a traditional form of Connection Admission Control (CAC) priority classification. The priority level recommendations proposed in this document strictly relate to the relative importance of traffic classes from this perspective; they do not reflect implementation specific priority definitions. For example, there are mechanisms utilizing Multi-Protocol Label Switching - Traffic Engineering (MPLS-TE) that define specific priorities such as Label Switched Path (LSP) setup priority, holding priority, and preemption priority [4]. Such mechanism-specific priority definitions do not apply to the recommendations in this document.

4 RELATED WORK

A significant amount of work on ETS requirements is ongoing in various standards bodies. A detailed list of such efforts can be found in the ATIS/PRQC Technical Report T1.TR.79-2003, *Overview of Standards in Support of Emergency Telecommunications Service (ETS)* [2]. An ATIS Technical Report originated by the PRQC committee documents the need for traffic prioritization from the perspective of emergency services [5]. ANSI standard T1.202-2004 developed by the ATIS Telecom Management and Operations Committee provides network management guidelines and recommendations under disaster conditions [6].

In the ITU-T, Recommendation E.361 [7] has progressed work on the definition of reliability and priority parameters for QoS service classes. This Recommendation also provides useful insights on the priority signaling across multiple networks. ITU-T Recommendation Y.1541 [8] provides a classification of IP communications services from the perspective of performance requirements. ITU-T Recommendation Y.1291 [9] presents a discussion on priority levels for CAC and service restoration functions in packet networks.

In the IETF Next Steps in Signaling (NSIS) Working Group, work is ongoing to define Quality of Service (QoS) modeling parameters in IP networks. Initial efforts include the use of priority parameters [10]. The goal of this effort is to eventually embrace QoS and priority parameters that apply to specific mechanisms such that these values can be signaled throughout an IP network. Also in the IETF, the label distribution for Traffic Engineering and QoS (and hence priority) can be accomplished via the Resource Reservation Protocol - Traffic Engineering (RSVP-TE) [11]. This protocol permits the creation of explicitly routed LSPs and provides fast rerouting, traffic and QoS specification, preemption, and other capabilities.

5 CAC PRIORITY PRINCIPLES

CAC policies provide the means to preferentially admit critical traffic flows into an IP network. For example, in an MPLS network, a higher priority service can be admitted by setting up an appropriate LSP in preference over a lower priority service by reserving the last available, minimum-level of bandwidth (called the "reserved bandwidth") for the higher priority service LSP set up [5]. The higher priority service only uses the reserved bandwidth for LSP setup when that is all the bandwidth left. In emergency conditions, when service network capacities are likely to be reduced, effective CAC mechanisms that recognize agreed upon priority services such as emergency communications, are critical to the successful setup and transmission of such services.

The following principles can be used for guidance in order to establish a set of priority levels for CAC functions in IP networks:

- ◆ *CAC Priority Lower Bound/Diversity of IP Services:* The evolution of IP networks is driven by the idea of convergence - the ability to transmit all types of communications traffic over IP backbones. Thus, service providers are increasingly planning the use of "converged" IP networks to carry real-time services such as Voice over IP (VoIP) as well as video, private data traffic (exemplified by VPN traffic), emergency traffic (VoIP, and in the future, data and video), in addition to today's "traditional" Best Effort services such as e-mail and web browsing. This suggests that simply categorizing bearer plane traffic as "emergency" and "other" may not be sufficient. Under such a two-level scheme, CAC policies may be likely to reject VPN and real-time VoIP traffic just as equally as Best Effort traffic in order to preferentially admit higher

priority traffic (e.g., ETS calls) under emergency conditions. This suggests that while two levels could serve as a lower bound for the number of bearer plane traffic CAC priorities, the actual number of levels should be higher. The goal is to ensure that, as far as possible, the maximum rejection for incoming traffic flows is borne by the Best Effort traffic class.

- ◆ *CAC Priority Upper Bound*: The advent of IP networking involved a single “Best Effort” class of service for simplicity. Subsequently, the ability of newer MPLS-based mechanisms can provide ways to distinguish different service types; however, these mechanisms do not suggest an arbitrarily large number of priority levels. For example, MPLS-based LSPs are assigned an EXP (experimental) bit value that may be used as a QoS indicator. There are 3 EXP bits and hence, eight possible QoS values can be assigned to an LSP. More significantly, DiffServ-aware MPLS Traffic Engineering (DS-TE) allows traffic to be classified into eight class types. Hence, up to eight potential EXP/QoS values can be assigned to these Class Types.
- ◆ *Emergency Traffic Priority*: Regardless of the number of CAC priority levels, emergency traffic such as ETS and E911 services should be assigned the highest available CAC priority value. As noted in the scope (also see clause 7), the ability to distinguish between types of emergency traffic is beyond the scope of this document.

6 RECOMMENDATION FOR CAC PRIORITY LEVELS

Based on the above principles, it is recommended that three CAC priority levels are sufficient for user plane traffic:

1. *High*: Emergency services (e.g., ETS and E911). Note that ETS can comprise real-time VoIP services as well as data and video services in the future.
2. *Normal*: Examples include real-time services (VoIP, video), VPN, and Data services. The selection of this priority class is expected to be determined by appropriate Service Level Agreements (SLA) between service carriers and customers for the desired service.
3. *Best Effort*: Examples include “traditional” Internet Service Provider (ISP) services (e-mail, web surfing). The selection of this priority class is expected to be determined by appropriate SLA agreements between service carriers and customers for the desired service. Note that this class of traffic can be of significant volume and can provide a cushion to protect more important high and normal priority services.

The goal of this classification is the following: under reduced network bandwidth conditions, high and normal priority traffic flows are given higher priorities of admission at the expense of best effort traffic. Further, under very severe emergency conditions where significantly large portions of a network are unavailable, high priority traffic flows are given higher priorities of admission over normal and best effort traffic.

It is expected that the vast majority of failure/congestion conditions can be successfully mitigated by the presence of large traffic volumes representing best effort ISP traffic. Simulation modeling on the use of the DS-TE model Maximum Allocation with Reservation (MAR) shows that three priority levels effectively meets this objective ^[12].

7 FLEXIBILITY

As stated in the scope, this document provides a broad classification of IP traffic types from the perspective of call/session admission into an IP network. It is recognized that each broad traffic class can comprise various types of traffic and that different types of treatment may be desirable for specific traffic types within a broad traffic priority class. The totality of different types of traffic within each class can vary depending on the type of services offered by individual service providers. Some examples are as follows:

- ◆ *High Priority Emergency Services:* The two service types within this class are ETS and E911 services. Further, ETS can comprise real-time VoIP services and, possibly, future data and video services. It is anticipated that E911 calls would be local in nature, whereas ETS can potentially involve the use of nationwide networking across multiple domains. The prospective mechanisms for successfully enabling these services will need to take the type of traffic as well as the service performance requirements into account.
- ◆ *Normal Priority Services:* This broad class of traffic entails all non-emergency services that require better than “Best Effort” criticality. Thus, real-time business and residential VoIP calls as well as business data services and VPN services can be lumped together here depending on customer requirements. The relative importance of these services will vary according to customer requirements for different service providers. Also, performance requirements will need to be addressed for enabling these service offerings.

Flexibility is therefore essential for service providers in determining different types of treatment for various traffic types within each broad traffic class. Appropriate SLA agreements can be used for services that span multiple carrier domains.

8 CONCLUSION

This document proposes three levels for CAC priority in the user plane for IP networks: *high*, *normal*, and *best effort*. It further proposes that the high priority level should be reserved for emergency services such as ETS and E911. Such an arrangement can enable the completion of end-to-end traffic flows over multiple networks of different technologies. For instance, GETS calls – originating over the PSTN or over wireless access networks – can be transported over an IP backbone as a high priority traffic flow, and vice versa. The next steps for the ATIS PTSC-SAC and PRSC committees include the mapping of call control messages (*e.g.*, SIP messages) into the defined user plane priority levels for IP services. The classification for non-emergency services (normal or best effort) can be determined in appropriate SLA agreements between service providers and their customers.

On a final note, it is noted that additional priority levels may be considered in the future depending on service requirements/needs as well as the availability of advanced and mature enabling mechanisms.

9 DEFINITIONS

9.1 Connection Admission Control: A set of actions/policies taken by the network at session set-up phase in order to accept or reject a packet flow.

9.2 Emergency Telecommunications Service: A service offering available on communications networks to facilitate the work of authorized emergency personnel in times of disaster, national emergency, or for executive/governmental communications relating to National Security/Emergency Preparedness (NS/EP).

10 ABBREVIATIONS AND ACRONYMS

ATIS	Alliance for Telecommunications Industry Solutions
BGP	Border Gateway Protocol
CAC	Connection Admission Control
DS-TE	DiffServ-Aware MPLS Traffic Engineering
ETS	Emergency Telecommunications Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector
LSP	Label Switched Path
MPLS	Multi-Protocol Label Switching
MPLS-TE	MPLS Traffic Engineering
NS/EP	National Security/Emergency Preparedness
NSIS	Next Steps in Signaling
OSPF	Open Shortest Path First
QoS	Quality of Service
SIP	Session Initiation Protocol
SLA	Service Level Agreement
VoIP	Voice over IP
VPN	Virtual Private Network

11 REFERENCES

- [1] Contribution T1A1/2003-160, "Communication from T1S1.7 to T1A1 Requesting Guidance on Priority Levels", June 2004.¹
- [2] T1.TR.79-2003, *Overview of Standards in Support of Emergency Telecommunications Service (ETS)*.²
- [3] Contribution T1S1/2003-384, "Proposal for ISUP to IP (SIP) Inter-working to support National Security and Emergency Preparedness (NS/EP)", May 2004.¹

¹ ATIS contributions are available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005; phone 202.628.6380.

² This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < <https://www.atis.org/docstore/default.aspx> >

ATIS-0100003

- [4] Contribution T1A1/2003-127R1, "Mechanisms for IP Priority Services and Standards Implications", P. S. Tarapore, *et al.*, T1A1 May 2004.¹
- [5] T1.TR.84-2004, *IP Network Traffic Priorities and ETS*.²
- [6] T1.202-2004, *Internetwork Operations - Guidelines for Network Management of the Public Telecommunications Network under Disaster Conditions*.²
- [7] ITU-T Recommendation E.361, *QoS Routing Support for Inter-working of QoS Service Classes Across Routing Technologies*, May 2003.³
- [8] ITU-T Recommendation Y.1541, *Network Performance Objectives for IP-Based Services*, May 2002.³
- [9] ITU-T Recommendation Y.1291, *An Architectural Framework for Support of Quality of Service in Packet Networks*, May 2004.³
- [10] IETF I-D draft-ash-nsis-nslp-qos-sig-proof-of-concept-00.txt, "NSIS Network Service Layer Protocol QoS Signaling Proof-of-Concept," J. Ash, *et al.*, February 2004.^{4, 5}
- [11] IETF RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, December 2001.⁶
- [12] IETF RFC 4126, *Max Allocation with Reservation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering & Performance Comparisons*, June 2005.⁴

³ This document is available from the International Telecommunications Union at < <http://www.itu.int/ITU-T/> >.

⁴ IETF I-Ds are available at < <https://datatracker.ietf.org/public/pidtracker.cgi> >; archived copies can be found on that site or < <http://www.potaroo.net/ietf/> >.

⁵ Reference [10] is expired, and an archive copy can be found at < <http://www.potaroo.net/ietf/> >.

⁶ This document is available from the Internet Engineering Task Force (IETF) at < <http://www.ietf.org> >.