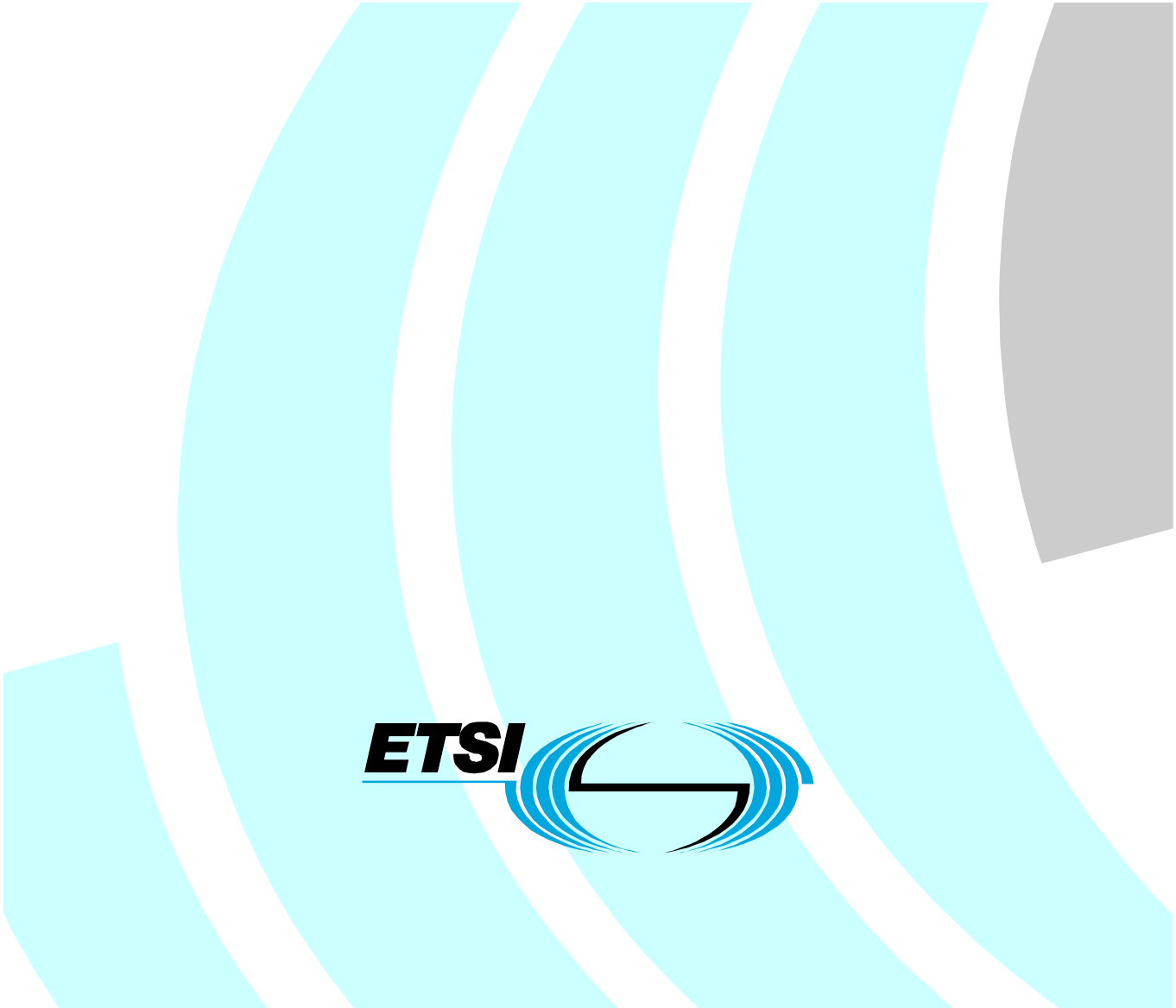
ETSI TR 102 157 V1.1.1 (2003-07)

Technical Report

Satellite Earth Stations and Systems (SES);
Broadband Satellite Multimedia;
IP Interworking over satellite;
Performance, Availability and
Quality of Service



Reference
DTR/SES-00083

Keywords
internet, broadband, satellite, QoS, performance, interworking, IP, multimedia, security, availability

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Introduction

The present document establishes a framework for specifying quality of service (QoS) requirements for Broadband Satellite (BSM) Networks based on the Internet Protocol (IP) suite of protocols and standards developed in ETSI and other bodies. It investigates how Internet standards that relate to quality can be adapted, translated or made transparent to satellite transmission protocols and equipment. It identifies new specifications to improve the efficiency of BSM systems in transporting Internet traffic with QoS. The original set of Internet protocols did not have to deal with variable link layer conditions, high asymmetry and higher delay that are characteristics of satellite networks. This needs to be taken into account when designing BSM to be integrally part of the public Internet.

In addition, since quality without ways to measure performance is irrelevant, the present document also investigates and proposes performance control and measurement mechanisms. Those will enable satellite and Internet service provider to establish how well the BSM network behaves with IP traffic. The recommended ETSI specifications will ensure end-to-end QoS and in turn wide acceptance of BSM in the Internet community.

1 Scope

The objectives of BSM IP QoS standardization are:

- to define what QoS is in the context of the BSM and how to measure it;
- to identify what QoS models are applicable to BSMs;
- to identify standardized performance metrics that can guarantee the performance of IP over the BSM; and
- to provide BSM services at the right level of QoS thus enabling a better utilization of BSM resources, in particular the scarce resources of the radio spectrum.

Hence, the scope of the present document is on the provisioning of Internet QoS over BSM networks. It will investigate how standardized QoS parameters and management mechanisms apply to BSMs and how to ensure that their required performance is met.

In addition, the scope of the present document encompasses:

- the identification of specific BSM architectures and the and how they provide quality of service;
- the definition of Internet service availability in the context of BSM and the establishment of end-to-end performance metrics;
- the identification and application of other ETSI technical specifications outside the BSM such as TIPHON and 3GPP;
- the identification of relevant standardization work in other standards bodies working groups such as the Internet Engineering Task Force (IETF) working groups on Integrated Services (Intserv), Differentiated Service (Diffserv), Internet Protocol Performance Metrics (IPPM) and Performance Implications of Link Characteristics (PILC), the International Telecommunications Union Study Groups (ITU SG) 2, 4, 12, 13 and 16, the Institute of Electrical and Electronic Engineers (IEEE) and finally, the Digital Video Broadcasting Internet Protocol Infrastructure Group (DVB IPI);
- the identification of satellite specific technical requirements for BSM quality of service, including service architecture, the use of standardized Internet protocols and extensions to satellite networking when and if needed; and
- the identification of satellite specific technical requirements for BSM performance and availability at the network layer.

The present document follows inputs from the following earlier reports in the BSM WG:

- TR 101 984 [11], "Broadband Satellite Multimedia: Services and Architectures";
- TR 101 985 [12], "Broadband Satellite Multimedia: IP over Satellite";
- TR 102 155 [13], "Broadband Satellite Multimedia: Addressing and routing"; and
- TR 102 156 [14], "Broadband Satellite Multimedia: Multicasting".

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TS 101 350: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2 (3GPP 03.64 version 8.9.0 Release 1999)".

[2] ETSI TS 123 107: "Universal Mobile Telecommunications System (UMTS); Quality of Service (QoS) concept and architecture (3GPP TS 23.107 version 5.7.0 Release 5)".

[3] Apostopoulos, G. et al.: "Quality of Service-based routing: A Performance Perspective", Proceedings of the ACM SIGCOM, 1998, pp. 17-28.

[4] ATM Forum: "User Network Interface (UNI) Signalling v.4.1", Document af-sig-0061.002, April 2002.

[5] ATM Forum 98/0828: "A Progress Report on the Standards Development for Satellite ATM Networks" November 1998.

[6] ETSI EN 300 726: "Digital cellular telecommunications system (Phase 2+) (GSM); Enhanced Full Rate (EFR) speech transcoding (GSM 06.60 version 7.0.2 Release 1998)".

[7] ETSI EN 300 961: "Digital cellular telecommunications system (Phase 2+) (GSM); Full rate speech; Transcoding (GSM 06.10 version 7.0.2 Release 1998)".

[8] ETSI EN 301 790: "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".

[9] ETSI EG 202 009-1: "User Group; Quality of Telecom Services; Part 1: Methodology for identification of parameters relevant to the Users".

[10] ETSI STF 214 Terms of References (ToR), November 2001.

[11] ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Services and Architectures".

[12] ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".

[13] ETSI TR 102 155: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP interworking over satellite; Addressing and routing".

[14] ETSI TR 102 156: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP interworking over satellite; Multicasting".

[15] ETSI TS 101 329-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 2: Definition of speech Quality of Service (QoS) classes".

[16] ETSI TS 101 329-3: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 3: Signalling and control of end-to-end Quality of Service (QoS)".

[17] ETSI TS 101 329-5: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 5: Quality of Service (QoS) measurement methodologies".

[18] Ferguson, P. & Huston, G.: "Quality of Service: Delivering QoS on the Internet and in Corporate Networks", John Wiley and Sons, January 1998.

[19] Floyd, S. and Jacobson, V.: "Random Early Detection Gateways for Congestion Avoidance", IEEE/ACM Transactions in Networking, V.1 N.4, August 1993.

[20] Huston, G.: "Internet Performance Survival Guide", Wiley, 2000.

[21] IEEE 802.1D: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - IEEE standard for local and metropolitan area networks - Common specifications - Media access control (MAC) Bridges", 1998 Edition (ISO/IEC 15802-3: 1998).

NOTE: http://standards.ieee.org/getieee802/download/802.1D-1998.pdf.

[22] IEEE 802.3 (2002): "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications".

NOTE: http://standards.ieee.org/getieee802/802.3.html.

[23] ITU-R Recommendation S.1424 (2000): "Apportionment of the Allowable Error Performance Degradations to Fixed Satellite Service (FSS) Hypothetical Reference Digital Path".

[24] ITU-R Recommendation S.1425 (2000): "Availability Objectives for a Hypothetical Reference Digital Path".

[25] ITU-T Recommendation SG 12 Contribution 37 (2001): "Draft New Recommendation G.QoSRQT - End-User Multimedia QoS Categories".

[26] ITU-T Recommendation Y.1540 (2002): "Internet protocol data communication service - IP packet transfer and availability performance parameters".

[27] ITU-T Recommendation Y.1541 (2002): "Network performance objectives for IP-based services".

[28] ITU-T Recommendation Y.1231 (2000): "IP Access Network Architecture".

[29] ITU-T Recommendation Y.1221 (2002): "Traffic control and congestion control in IP based networks".

[30] ITU-T Interim Rapporteur Meeting Report, Y.SatIP-qos (2002): "IP QoS for Satellite-Terrestrial Networks".

[31] ITU-T Recommendation X.605 (1998): "Information technology - Enhanced Communications Transport Service Definition".

[32] ITU-T Recommendation X.606 (2001): "Information technology - Enhanced communications transport protocol: Specification of simplex multicast transport".

[33] RFC 1155 (1990): "Structure and Identification of Management Information for TCP/IP-based Internets".

[34] RFC 1633 (1994): "Integrated Services in the Internet Architecture: an Overview".

[35] RFC 1944 (1996): "Benchmarking Methodology for Network Interconnect Devices".

[36] RFC 2001 (1997): "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms".

[37] RFC 2018 (1996): "TCP Selective Acknowledgment Options".

[38] RFC 2205 (1997): "Resource ReSerVation Protocol (RSVP)".

[39] RFC 2210 (1997): "The Use of RSVP with IETF Integrated Services".

[40] RFC 2211 (1997): "Specification of the Controlled-Load Network Element Service".

[41] RFC 2212 (1997): "Specification of Guaranteed Quality of Service".

[42] RFC 2330 (1998): "Framework for IP Performance Metrics".

[43] RFC 2414 (1998): "Increasing TCP's Initial Window".

[44] RFC 2474 (1998): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[45] RFC 2475 (1998): "An Architecture for Differentiated Services".

[46] RFC 2488 (1999): "Enhancing TCP over Satellite Channels using Standard Mechanisms".

[47] RFC 2597 (1999): "Assured Forwarding PHB Group".

[48] RFC 2598 (1999): "An Expedited Forwarding PHB".

[49] RFC 2676 (1999): "QoS Routing Mechanisms and OSPF Extensions".

[50] RFC 2678 (1999): "IPPM Metrics for Measuring Connectivity".

[51] RFC 2679 (1999): "A One-way Delay Metric for IPPM".

[52] RFC 2680 (1999): "A One-way Packet Loss Metric for IPPM".

[53] RFC 2681 (1999): "A Round-trip Delay Metric for IPPM".

[54] RFC 2702 (1999): "Requirements for Traffic Engineering Over MPLS".

[55] RFC 2748 (2000): "The COPS (Common Open Policy Service) Protocol".

[56] RFC 2914 (2000): "Congestion Control Principles".

[57] RFC 3031 (2001): "Multi-protocol Label Switching Architecture".

[58] RFC 3077 (2001): "A Link-Layer Tunnelling Mechanism for Unidirectional Links".

[59] RFC 3084 (2001): "COPS Usage for Policy Provisioning".

[60] RFC 3135 (2001): "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradation".

[61] RFC 3155 (2001): "End-to-end Performance Implications of Links with Errors".

[62] RFC 3168 (2001): "The Addition of Explicit Congestion Notification (ECN) to IP".

[63] RFC 3261 (2002): "SIP: Session Initiation Protocol".

[64] RFC 3357 (2002): "One-way Loss Pattern Sample Metrics".

[65] RFC 3448 (2003): "TCP Friendly Rate Control (TFRC): Protocol Specification".

[66] TIA/EIA Committee TR-34.1, Telecommunications Systems Bulletin: "Satellite ATM Networks: Architectures and Guidelines", ANSI/TIA/EIA/TSB 90, May 1998.

[67] Wiles, A.: "SIP: What is it and is it important to ETSI?" ETSI PTCC STF Colloquium, 12 February 2003.

[68] ETSI ETR 309: "Special Mobile Group (SMG); Vocabulary for the Universal Mobile Telecommunications System (UMTS) (UMTS 01.02)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

availability (measure): percentage of the time the network performs at nominal capacity

NOTE: It is also defined as the probability that the network will provide a satisfactory service on demand.

availability (performance): ability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided

bearer service: service that provides the transmission capability between access points

Best Effort (BE) service: service which offers no QoS guarantees, just end-to-end connectivity

NOTE: When using queuing to prevent congestion BE queues are always the first ones to experience packet drop.

Bit Error Ratio (BER): number of bits in error as measured at the BSM to host interface measured over a specified amount of time

bit rate: information rate at the level of the application

BSM bit rate: information rate before FEC but after segmentation and encapsulation

Class Of Service (COS): The COS defines a way to divide traffic into separate categories (classes) to provide Diffserv to each class within the network.

connection oriented: communication method in which communication proceeds through three well-defined phases: connection establishment, data transfer, and connection release

connectionless: communication method that allows the transfer of information between users without the need for connection establishment procedures

control plane: The control plane has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections.

data link layer: second layer of the OSI model it provides connectivity between segments of the network (bridging); in addition the data link may perform session control and some configuration

Data Transfer Unit (DTU): fixed size entity after segmentation and encapsulation but before FEC i.e. ATM cell, MPEG packet**,** other fixed length unit

delay: The delay measures the latency between the time a packet crosses the ingress of the network (enter the SI part of the transmitting ST) to the time it crosses the egress of the network (leaves the SI part of the receiving ST).

delay variation: The delay variation measures the differences in delay between successive packet arrivals (of the same flow) at the egress of the network. Delay variation can be reduced by means of buffering, although at the expense of adding additional delay.

Differentiated services (Diffserv): Those are based on statistical (aggregate flows) guarantees and results in "soft" QoS. Using packet markings (code points) and queuing policies it results in some traffic to be better treated or given priority over other (use more bandwidth, experience less loss etc.).

fairness: Fairness implies that all data flows requiring service will get that service based on their specific requirements.

flow: A flow can be defined in a number of ways. One common way refers to a combination of source and destination addresses, source and destination socket numbers, and the session identifier. It can also be defined more broadly as any packet from a certain application or from an incoming interface.

Grade Of Service (GOS): in telephony, the quality of service for which a circuit is designed or conditioned to provide, e.g. voice grade or program grade

guaranteed services: using RVSP and integrated services this results in deterministic reservation of network resources for specific traffic

goodput: the actual information rate delivered to the application

Internet: the public datagram global network supporting the internet protocol (IP)

internet: any network that supports IP

management plane: plane that provides two types of functions, namely layer management and plane management functions:

- **Plane management functions:** performs management functions related to a system as a whole and provides co-ordination between all the planes

NOTE: Plane management has no layered structure.

- **Layer Management functions:** performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities

NOTE: Layer Management handles the Operation And Maintenance (OAM) of information flows specific to the layer concerned.

multicast: communication capability which denotes unidirectional distribution from a single source to a number of destinations

network operator: The network operator is responsible for managing the network services provided over the satellite resources. These resources may be unique or represent a sub-network in the operator's overall network.

offered load: the traffic presented to the ingress of the network

packet: IP packet of variable size

packet loss: the number of IP packets lost to queuing or transmission

Quality of Service (QoS): the ability to segment traffic or differentiate between traffic types in order for the network to treat certain traffic differently from others. QoS encompasses both the service categorization and the overall performance of the network for each category. It also refers to the capability of a network to provide better service to selected network traffic over various technologies and IP-routed networks that may use any or all of the underlying technologies. QoS is defined as the collective effect of service performances which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as: - service operability performance; - service accessibility performance; - service retainability performance; - service integrity performance and other factors specific to each service.

QoS parameters: parameters that will be specified or monitored to ensure QoS

satellite operator: The satellite operator is responsible for the bulk transport services. Those services are provided to the network operator.

service levels: actual end-to-end QoS capabilities of the network which will enable it to deliver a service needed by a specific mix of network traffic

NOTE: The services themselves may differ in their level of QoS.

Service Level Agreement (SLA) (Subscriber and Service Provider): The SLA between a SP and its subscriber is characterized by the choice of one data transfer capability and the allocation attribute related to this transfer capability. The SLA is agreed upon by the subscriber at the initiation of the contract with the SP and will remain the same for all the contract duration.

Service Level Agreement (SLA) (SP and ANO): The SLA between a Service Provider and an Access Network Operator is usually characterized by a forward link guaranteed capacity for SP aggregated traffic expressed in kb/s and a return link guaranteed capacity for SP aggregated traffic expressed in kb/s. It can also include other elements related to traffic policy and availability.

service provider: interface between the customers (i.e. the subscribers and the users) and one or more network operators

NOTE: The service provider may obtain services from multiple network operators and may offer a combined service to the customers. The service provider is responsible for all aspects of the customer service from installation, to maintaining the quality of service during normal operation, to billing the customers for network usage.

subscriber: entity that enters into a service contract with the service provider

NOTE: A single subscriber may support one or several users with a single contract (e.g. a large company subscriber may subscribe for services to several hundred users).

throughput: parameter that defines the effective network data transfer rate in bits per second (bps) for a particular service

NOTE: It is measured from ingress interface to egress interface. In the BSM it is the information rate after decoding but before re-assembly.

user plane: The user plane has a layered structure and provides for user information flow transfer, along with associated controls (e.g. flow control, recovery from errors, etc).

user: the entity that uses the network services provided by the subscriber

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
8-PSK	Octagonal Phase Shift Keying
ABC	Adaptive Bandwidth Control
ABR	Available Bit Rate
AC	Admission Control
ACK	ACKnowledgment
ADSL	Asymmetrical Digital Subscriber Loop
AF	Assured Forwarding
API	Application Program Interfaces
APPS	Applications
AQM	Active Queue Management
ATM	Asynchronous Transfer Mode
B	Byte = 8 bits
BB	Bandwidth Broker
BE	Best Effort
BER	Bit Error Ratio
BGP	Border Gateway Protocol
B-ISDN	Broadband ISDN
BoD	Bandwidth on Demand
BPM	B(SM) Protocol Manager
BSM	Broadband Satellite Multimedia
CAC	Connection Admission Control
CBR	Constant Bit Rate
CDMA	Code Division Multiple Access
CLP	Cell Loss Priority
CLS	Controlled Load Service
COPS	Common Open Policy Service
COS	Class of Service
COS	Class Of Service
COTS	Custom Off The Shelf
CR	Constant Rate
CRC	Cyclic Redundancy Code
cwnd	congestion window (TCP)
DAMA	Demand Assigned Multiple Access
DBP	Delay Bandwidth Product
DBR	Deterministic Bit Rate
DBW	Dedicated BandWidth
DCCP	Datagram Congestion Control Protocol
Diffserv	Differentiated Services
DOCSIS	Data Over Cable Service Interface Specification
DSCP	Differentiated Services CodePoint
DSL	Digital Subscriber Loop
DTU	Data Transfer Unit (with CRC)
DVB	Digital Video Broadcast
DVB-RCS	DVB Return Channel for Satellite
DVB-S	Digital Video Broadcast via Satellite
e.i.r.p.	effective isotropic radiated power
E_b/N_0	bit Energy to Noise ratio
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
EPD	Early Packet Discard
FEC	Forward Error Correction

FSAN	Full Service Access Network
FSS	Fixed Satellite Service
FTP	File Transfer Protocol
G/T	antenna Gain-to-system noise Temperature ratio
GEO	Geostationary Earth Orbit
GOS	Grade Of Service
GS	Guaranteed Service
GSO	GeoStationary earth Orbit
HDR	HeaDeR
HRDP	Hypothetical Reference Digital Path
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Internet Draft
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
Intserv	Integrated services
IP	Internet Protocol
IPDV	IP packet Delay Variation
IPER	IP packet Error Ratio
IPLR	IP packet Loss Ratio
IPMA	Internet Performance Measurement and Analysis
IPPM	Internet Protocol Performance Metrics
IPR	Intellectual Property Rights
IPSec	IP Security
IPTD	IP packet Transfer Delay
IPV4/V6	Internet Protocol Version 4/6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication sector
ITU-T	ITU Telecommunication standardization sector
IWU	InterWorking Unit
kbps	kilo bit per second
kBps	kilo Byte per second
L2	Layer 2
LAN	Local Area Network
LEO	Low Earth Orbit
LISP	Lightweight Interlayer Signalling Protocol
LSP	Label Switched Path
MAC	Medium Access Control
Mbps	Megabits per second
MBS	Mean Burst Size
MEGACO	MEdia GAteway COntrol protocol
MF-TDMA	Multi-Frequency TDMA
MIB	Management Information Base
MPEG	Moving Pictures Expert Group
MPLS	MultiProtocol Label Switching
ms	milli-second
NANOG	North American Network Operator Group
NCC	Network Control Centre
NLANR	National Laboratory for Applied Network Research
NSAP	Network Status Advertisement Protocol
NSIS	Next Steps In Signalling
OAM	Operation And Maintenance
OBC	OnBoard Controller
OBP	OnBoard Processor
OBS	OnBoard Switch
OSI	Open System Interconnection
PCR	Peak Cell Rate
PDP	Policy Decision Point
PDU	Protocol Data Unit

PEP	Policy Enforcement Point (Diffserv, COPS)
PEP	Performance Enhancing Proxy
PHB	Per Hop Behaviour
PILC	Performance Implications of Link Characteristics
ping	packet internet groper (command)
PLR	Packet Loss Ratio
POP	Point Of Presence
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RED	Random Early Discard
RESV	RESerVation
RFC	Request For Comments
rmon	remote monitoring (command)
RMS	Root Mean Square
RSM	Regenerative Satellite with satellite return and Meshed topology
RSVP	ReSerVation Protocol
RTO	Retransmission Time-Out
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
RTT	Round Trip Time
SA	Source Address
SAP	Satellite Access Point
SBW	Statistical BandWidth
SD	Satellite Dependent
SDAF	Satellite Dependent Adaptation Functions
SDP	Session Description Protocol
SDU	Service Data Unit
SES	Satellite Earth Stations & Systems
SI	Satellite Independent
SIAF	Satellite Independent Adaptation Functions
SIP	Session Initiation Protocol
SI-SAP	Satellite Independent-Service Access Point
SLA	Service Level Agreement
SLC	Satellite Link Control
SMAC	Satellite Medium Access Control
SMTP	Simple Mail Transfer Protocol
SNAL	Satellite Network Adaptation Layer
SNMP	Simple Network Management Protocol
SP	Service Provider
SPHY	Satellite PHYsical
ssthresh	slow start threshold (TCP)
ST	Satellite Terminal
STF	Special Task Force
TBD	To Be Determined
TBF	Temporary Block Flow
TC	ETSI Technical Committee
TCP	Transport Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFI	Temporary Flow Identity
TFRC	TCP Friendly Rate Control
TIA	Telecommunications Industry Association (US)
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TR	Technical Report
TRIGTRAN	TRIGgers for TRANsport
TSS	Transparent Satellite with satellite return and Star topology
TTL	Time To Live

UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UNI	User to Network Interface
URI	Uniform Resource Identifier
URL	Universal Resource Locator
VBR	Variable Bit Rate
VLAN	Virtual LAN
VoIP	Voice over IP
VP	Virtual Path
VP	Virtual Path
VPN	Virtual Private Network
VR	Variable Rate
WG	Working Group
WRED	Weighted RED

4 Overview

QoS and performance aspects cover a wide range of networking topics. In order to focus on BSM specifics the present document addresses only those aspects that impact BSM architectures or are impacted by BSM architectures. In addition, the present document combines the contributions of a number of standardized bodies in each clause. Each topic is discussed in more detail in a separate clause. Table 1 lists all the clauses together with a brief description of the contents of each clause. The reader is assumed to know the basics of the Internet Protocols; however the appendices contains the IP header formats essential for understanding QoS. This note is also organized by layers, as proposed by the BSM stack of protocols. Another organization could have followed a more functional approach based on:

- admission control;
- end-to-end signalling (connection set-up);
- traffic forwarding; and
- policy-based control.

All these topics are nevertheless addressed as layer 3 or above functions in clauses 6 and 7.

Table 1: QoS and Performance

Topic	Clause	Description
BSM Architectures	5	What are the major BSM architectures and how these architectures influence QoS and performance management.
BSM QoS Management	6	A review of standardized QoS model and functions and how the BSM systems can accommodate these functions.
BSM Performance Management	7	A review of standardized performance measures and traffic models and how the BSM system performance related to these parameters.
BSM Protocol Manager	8	An introduction to the management software necessary for QoS and performance.
Recommendations	9	What specifications should ETSI develop in order to ensure that BSMs can support QoS under measurable and consistent performance.

5 Introduction

5.1 IP over BSM

The Internet suite of protocols (IP) in BSM networks faces some challenges that may or may not be shared by terrestrial wireline networks. Like the cellular networks, bandwidth is scarce, hence has to be managed carefully. Like some radio networks, availability of network resources can be low due to weather events. Delay is usually high and can be made worse by the use of bandwidth on demand or by repetitive error correction methods. Even when error-free, the delay bandwidth product of the BSM is usually high, like in optical networks but for different reasons, which is a throughput issue on reliable protocols like TCP. What characterizes BSM is that they are facing all these challenges together. The BSM network designer must use means to ensure that quality of service can still be offered at a level of performance and availability that make BSMs compelling for IP services.

5.2 Quality of Service

A network with QoS support provides certain priorities and guarantees to specific network traffic. These include but are not limited to: dedicated bandwidth controlled or managed jitter and latency for some real-time and interactive traffic, and predictable end-to-end loss characteristics. These provisions must be made in such a way that ensures fairness amongst different flows: priority for one or more flows in a class should not necessarily imply that other flows suffer and that lower priority flows never get service. QoS parameters are essentially set by applications and may also be customer-related. It is the role of performance monitoring to ensure that the QoS parameters are met and to enforce appropriate traffic engineering practices.

The implementation of a QoS framework essentially involves a number of networking functions:

1) application level: QoS parameter specification and techniques for coordinating QoS from end-to-end across the different network elements;

2) system level: packet marking, queuing, scheduling, and traffic-shaping tools that are provided within the network access devices and when appropriate at the layer 2 adaptation; and

3) performance management level: QoS policy management and accounting/billing functions that control the traffic across a subnet or a whole network.

The first element sets the goals for the other two. System level QoS relates the most to the underlying technologies and is particularly impacted by satellite technology. Performance management concerns the BSM operator. It specifies the policy management functions that in turn define how traffic enters the satellite network, under which conditions and at what cost for the operator.

BSM Quality of Service (BSM QoS) is defined as the QoS that applies to the BSM Bearer Services. These are the services that the BSM network operator offers to its customers, who pay for the quality they get. Figure 1 [12] shows the position of the BSM bearer service in the BSM architecture.

QoS management in the BSM must be based on some guiding principles that include:

- explicit admission control for those services requiring hard guarantees;
- minimization of packet loss due to buffer overflow or link errors;
- minimization of network idleness to ensure that resources are used and generate revenues; and
- fairness in the allocation of resources to requesting terminals and sessions within terminals.

The present document only considers QoS, performance and availability over a BSM. It is understood that the overall end-to-end performance and availability experienced by the end users will also be influenced by the other networks attached to the BSM. In particular some QoS parameters, packet marking and end-to-end Service Level Agreements may not be under the control of the BSM operator. When applicable those impacts will be identified in the appropriate clause.

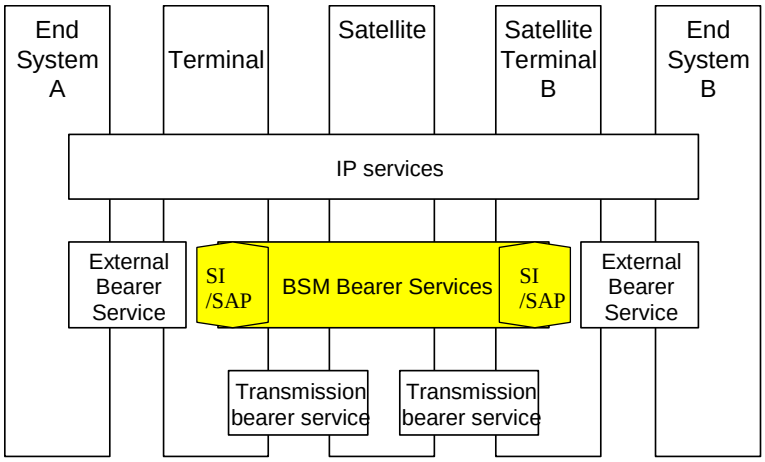


Figure 1: BSM bearer services [12]

5.3 BSM use cases

As defined in TR 101 984 [11], the BSM offers a general IP service that needs to evolve with the changes in the Internet. In the current context of the present document the use cases include but are not limited to:

- point to point connectivity;
- Internet access;
- content distribution; and
- real time multimedia streaming.

These use cases are shared amongst all current projects of the Special Task Force (STF) as well as having been addressed in both the Architectures [11] and Internet Protocol [12] TRs.

6 BSM architectures impacts on Quality of Service & performance

6.1 BSM systems

BSM architectures will have an effect on the behaviour of Internet Protocols (IP). In turn, if IP protocols perform poorly over a certain BSM, overall resource utilization can be low and wasted or the services relying on those protocols will experience outings or degraded quality. BSM QoS involves many layers of the protocol stack from the application protocol to the transport protocol and to data link protocols, from router buffer size, to queuing discipline and proxy. While a BSM shares a number of features with other systems it does have the specificity of dealing with long delays and bandwidth scarcity at the same time. It also needs to ensure that methods that protect the integrity of the BSM air interface do not make QoS impossible to manage by introducing unwanted delays. This clause identifies how the overall BSM architecture and environment will influence the quality experienced by applications using the IP suite of protocols.

BSM systems are composed of a space segment, of one or more satellites, and of a ground segment made of a Network Control Centre (NCC), of gateways and of individual Satellite Terminals (STs) (figure 2). Depending on the type of payload in the satellites different network architectures are made possible.

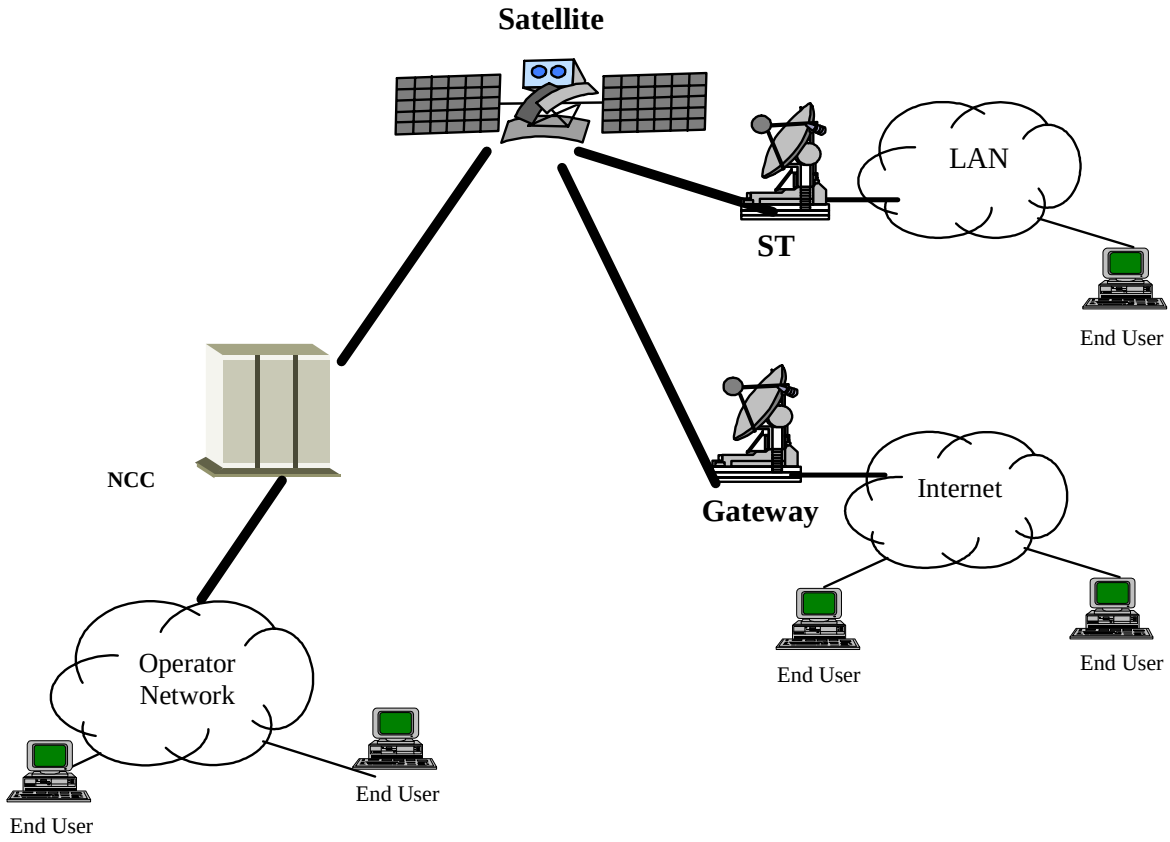


Figure 2: Generic BSM system

6.1.1 Transparent system

A BSM with a non-regenerative payload (a repeater) is commonly called a "bent-pipe system" or transparent system. This system does not terminate any layers of the BSM protocol stack in the satellite. The satellite simply repeats the signals from the user links to the feeder links transparently. With this system (which can use global and spot beams) the communications between an ST and the Internet are done via a gateway terminal attached to the Internet. The forward channel uses the satellite transmission. However, the return channel can use a number of technologies (e.g. satellite, phone or DSL network etc). This system is mainly used for access as it requires double satellite hops for ST to ST communications. In this system all most network functions are performed by the NCC.

6.1.2 Regenerative satellites (OBP)

A regenerative satellite offers bridging or network functionality in the satellite. Usually, this added functionality is to maximize the efficiency of multi-beam satellites and to improve allocation of spectrum resources on the uplink. In general the OnBoard Processor (OBP) uses an OnBoard Switch (OBS) to send BSM cells from beam to beam (digital switching). An OnBoard Controller (OBC) manages the uplink and downlink resources as well as some performance management onboard. In this system the Network Control Centre (NCC) is used for overall coordination, non real time resource management and network management. This system enables single-hop ST to ST (peer to peer) communications while still enabling access when required.

6.1.3 Constellations

While not the focus of this note, constellations of BSMs of different types can also be under consideration.

6.2 Network architectures

The use cases are provided by BSMs using three main network architectures that support point to point, multicast and broadcast services, namely:

- access network;
- content distribution to the edge; and
- core network.

A BSM network can support all three scenarios. However, the present document will give priority to issues related to the first two scenarios, namely access network scenarios and content distribution to the edge. This is because it does not specifically address multicast services where the BSM can play an important core role. In unicast services the data rates usually associated with core networks are above those offered by BSMs by orders of magnitudes (terabits per seconds on optical core networks).

6.2.1 BSM protocol stack

The BSM protocol stack [11], following the traditional OSI model, is shown in figure 3. QoS and performance will be defined and measured at the main interface between layers.

The SI/SAP interface plays an important role in performance monitoring. It is at that interface that satellite specific performance is translated into higher layer protocol semantics and that applications performance requirements are used to control the satellite specific functions.

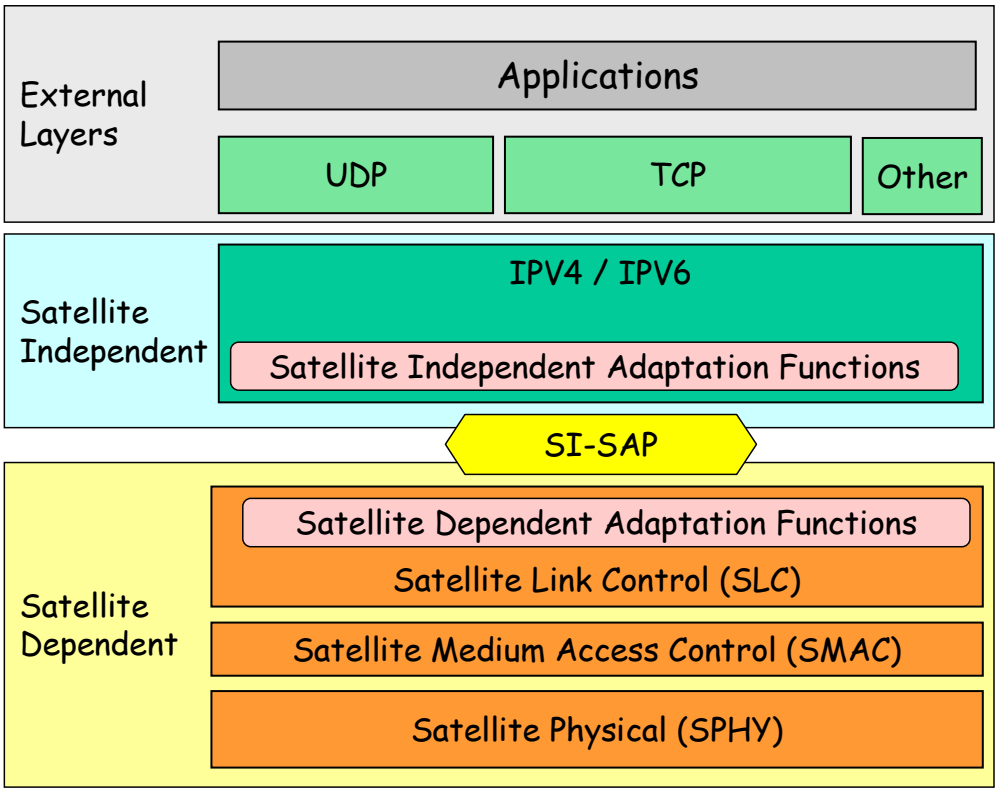


Figure 3: Protocol architecture [11]

The two main layers for QoS management are the Satellite Independent and Satellite Dependant layers. Within each layer some user plane, control planes and management plane function will be defined for QoS:

- user plane: packet marking and forwarding based on established policies;
- control plane: signalling and overall queue management; and

- management plane: admission/congestion/flow control parameters, packet sampling, and statistics gathering.

Depending on the supported model for QoS (Intserv, Diffserv or both) different functions and parameters can be used. Details are provided in clause 7.

6.2.2 BSM topology

A BSM network may support either a mesh or star topology as defined in the Services and Architectures TR 101 984 [11]:

- a star network topology is defined by the star arrangement of links between the Hub station (and Gateway) and multiple Remote stations. A Remote station can only establish a direct link with the Hub station and cannot establish a direct link to another Remote station. A star topology can be used to provide mesh connectivity by establishing an indirect link between Remote stations via the Hub station;
- a mesh network is defined by the mesh arrangement of links between the stations, where any station can link directly to any other station. The star topology can be considered as one special case of the mesh topology.

A BSM network may use either a non-regenerative or a regenerative system and various combinations of space segment and ground segments.

6.2.2.1 Access network

The access network as the name indicates allows the users connected to a ST to "access" the Internet (or other network) via a gateway. It uses a star topology and can be realized over both with bent pipe and OBP satellites (figures 4 and 5).

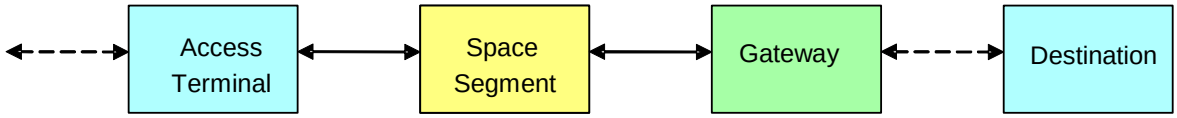


Figure 4: Simplified access network architecture

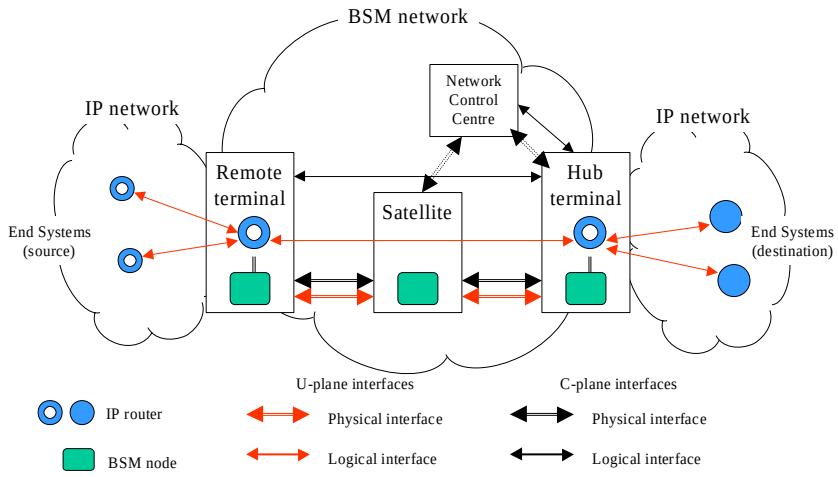


Figure 5: Access BSM [11], [12]

6.2.2.2 Meshed network

A meshed network enables peer to peer connectivity (figure 6). While in principle it can be realized over a bent pipe satellite it is more efficient over OBP architectures (figure 7) because of the impact of the double hop on a bent-pipe on low latency services.

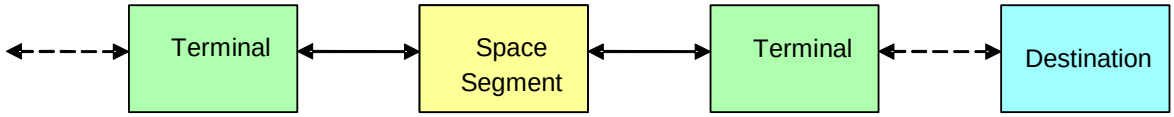


Figure 6: Simplified meshed network architecture

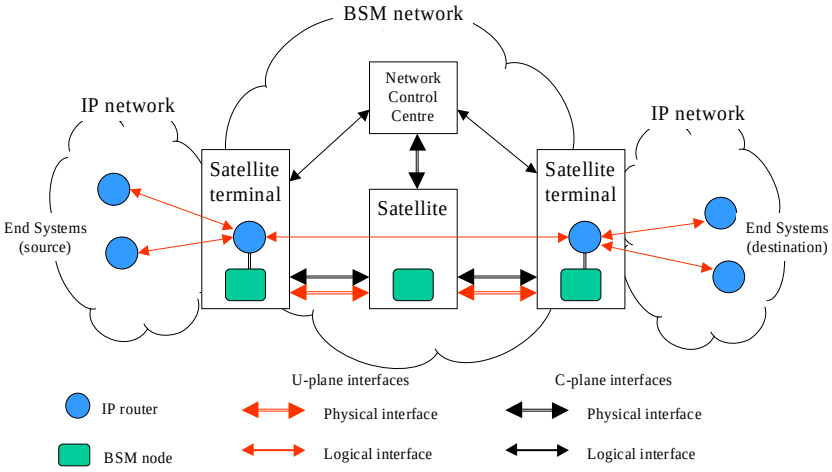


Figure 7: Meshed BSM [11], [12]

6.3 QoS and performance aspects

The BSM architecture defines which system element is involved in QoS and dictates some constraints on the level of performance. The BSM does not specify the QoS requirements: the applications that potentially cross a number of subnetworks define the QoS parameters and the required performance levels. The goal of the BSM segment will be to comply with (at least) the minimal service requirements.

BSMs may have certain disadvantages when compared to fibre channels (e.g. cannot be easily repaired, rain fades, etc.), but they also offer great advantages over terrestrial links that can be taken advantage of in QoS management. Broadcast capability, essential for multicast, and the large geographical coverage of BSMs means that the same QoS services may be offered to users in remote areas or countries that have little terrestrial infrastructure. There are other well known factors that are inherent to BSM that influence QoS. In particular, the BSM manager has control over the BSM: to enter the BSM subnetwork any packet will cross an interface directly controlled by the BSM. While QoS will be studied in detail in clause 7 it is important to highlight some of architecture impacts here.

6.3.1 Void

6.3.1.1 Network topology

For access networks using a star topology, the QoS management and performance monitoring are located in the gateway and the terminals. The terminal functions will probably be limited to packet level and local functions. The gateway will implement more complex management schemes and centralize the BSM management. As mentioned in clause 7.2.3 double hops should be avoided on all functions, as some QoS parameters will not be met with long delays.

For the mesh topology, the same can apply except that now every ST is a gateway and the satellite payload can become an actor in performance monitoring and QoS management. While no active QoS management in the space segment is needed, at minimum the status information from the payload as well as more advanced queue management functions can be implemented. This gives added information for the connected networks in terms of what is available in the BSM and at which performance level.

The type of return channel can influence how QoS will be provided on the BSM. When no return channel is available then the BSM QoS on the forward channel will mainly be at the link level (coding, power etc.). The use of a terrestrial narrowband or broadband return channel leads to hybrid schemes. The QoS depends on the terrestrial segment as well as the space segment and consist of two different management paths. A satellite return channel based protocol like DVB-RCS puts the QoS over the BSM totally in the hands of the BSM manager and can lead to specific BSM approaches at layer 2 (BSM as a bridge) and layer 3 (BSM as a router). This last scenario is the focus of most of the present document.

In addition the higher number of satellites in a constellation may lead to multipath routing, out of order deliveries and added delay variations. Overall, one way to avoid some of those QoS issues in the constellation is to use hybrid BSM-terrestrial schemes. In such a scheme, the satellite is used to get to the nearest Point of Presence (POP) or service provider; then the terrestrial network is used to reach the destination. Hence delay variation is minimized and routing complexity and the risk of multipath routing greatly reduced.

6.3.1.2 Orbit and delay

Delay over the BSM is due to the time (at the speed of light) needed to reach the orbit of a BSM space segment. Most BSMs are located at the Geostationary Orbit (GSO) with an altitude of approximately 36 000 km. The propagation time for a radio signal to travel twice that distance from a point directly below the satellite is 239,6 ms. It will be higher for STs located somewhere else and it is generally accepted that the "mean" delay is about 250 ms for 1 hop. The propagation delay for a message and the corresponding reply defined as one round-trip time or RTT will be at least 500 ms to 600 ms. It is important to note at this point that Low Earth Orbit (LEO) BSMs are not currently addressed in this note. Their delay is significantly lower (less than 100 ms) but they can experience large delay variations.

Another impact of the BSM delay is a large Delay×Bandwidth Product. The Delay×Bandwidth Product (DBP) is the product of the RTT and the available bottleneck bandwidth. It defines the amount of data a protocol should have "in flight". Large DBPs are not specific to BSM as this property is also shared by fibre networks (small delays but huge bandwidth); they require special attention to ensure that resources are fully utilized (see clause 8.3).

The RTT can and will be increased by other delays in the network including transmission in other links of the path, queuing delays in routers and gateways and encoding and bandwidth allocation delays. For RSMs, that include on-board processing and queuing, additional delay may be added. Delay creates long feedback loops that have an impact on QoS for those services requiring real-time response or interactivity (e.g. telnet) and also degrades the performance of flow and congestion control algorithms used by protocols like the Transport Control Protocol (TCP). It is a good practice to perform an end-to-end delay budget (table 2) over the BSM in order to verify if the design is compliant to the application requirements.

Table 2: Example of delay budget for a TSS type BSM

Segment	Value (ms)
Source to ST	10 ms
Segmentation/queuing	5 ms
BOD	575 ms (RTT of 500 ms plus processing time)
Transmission	250 ms
Re-assembly/queuing	5 ms
ST to destination	0 (destination attached to the ST)
Total:	845 ms This figure will get higher with the addition of login, authentication and/or address resolution delays

6.3.1.3 Channel noise

For BSMs most frequency bands under consideration include Ku (12 GHz to 15 GHz) and Ka (20 GHz to 30 GHz) meaning both large bandwidth but also increased transmission disturbances due to weather and atmospheric events: wind that can move ST antennas, rain that induces large fades and scintillation that causes interference. The results are usually error bursts (or reduced bandwidth) that will lead to packet loss. In addition, for mobile terminals, shadowing and other intermittent events will lead to reduced performance.

The bit error ratio (BER) is measured over a period time as the number of bits in error compared to the overall number of bits transmitted. Depending on the type of system this time measurement can vary and is specified by the ITU-R. The typical BER for a BSM is on the order of 1 error per 10 million bits (1×10^{-7}) or less with the use of advanced error control coding. Obviously, this is measured when the service is available as some deep fades may result in total outage hence a much higher loss. This what makes a wireless system different from a wired one: the variable availability due to fades and outages.

But the low BER of the BSM when operational means that BSM error performance approaching fibre is now a reality and the "high noise" of satellite may not be a problem all the time. New systems will use adaptive coding and modulation (such DVB-S2). The selection of link parameters will influence link quality, capacity and latency. While large interleaver blocks, concatenation and turbo encoding are beneficial to reduce errors, they also delay packets which can be harmful on end-to-end latency and thus induce loss at higher layers. In addition, as will be seen in clause 8.4.3.2.3, residual errors will have to be dealt with. Finally, some legacy systems may exhibit higher BERs.

6.3.1.4 Bandwidth

It is well know that spectrum resources (as well as the possible number of satellites in a certain frequency band) are very limited. QoS management requires bandwidth for signalling, maintenance and service differentiation. The BSM cannot allocate bandwidth that does not exist hence tight bandwidth management is central to BSM QoS. Any QoS mechanism must ensure that bandwidth is available for high priority (or high revenue generating) services even if it means dropping lower level sessions in times of high load or high noise. Depending on the frequency band the amount of bandwidth available to an application will be limited and may be compounded by other impairments such as delay or loss. But, as seen in table 3, illustrative of some data services, the rates that are offered by current and proposed BSMs are well above most of terrestrial offerings making them competitive.

Table 3: Illustrative rates for selected Internet technologies

Type	Uplink	Downlink
GPRS	14 kbps	28 kbps to 64 kbps
Dial-UP	56 kbps	56 kbps
ISDN Standard	64 kbps	64 kbps
ADSL	256 kbps	512 kbps
BSM (generic)	kbps to Mbps	> 34 Mbps

6.3.1.5 Access schemes

The use of a certain access scheme especially on the uplink also has some impact on the BSM QoS. The focus here is on time division and code division.

6.3.1.5.1 TDM(A) and MF-TDMA

Time division access schemes impact overall QoS. There are issues about how time slots (being variable like in DVB-RCS or fixed) can be allocated to requesting session. This is totally under the control of the communication system designers. However, some systems are unable to jump across frequencies in adjacent time slots limiting the number of slots per frame allocated to a single terminal. This results in less allocated bandwidth and either higher delay or higher loss (waiting packets get discarded). In addition the reservation can take away valuable bandwidth. Finally the amount of data sent per time slot will influence the level of segmentation of the IP packets hence the level of fragmentation IP packets will experience with impacts on higher layer protocols.

6.3.1.5.2 CDMA

CDMA is not currently deployed in BSM networks but has been envisaged as an access method for ST return channels. However, most CDMA proposals in the 3G/4G mobile communication were developed strictly for voice and do not support broadband multimedia adequately. For example there is no packet scheduling algorithms that are inherently part of CDMA hence making it difficult to prioritize packets. There have been proposals for combined TDMA/CDMA hybrids that may resolve some of the scheduling of CDMA. In addition, multi-code approaches have also been investigated where some "good" codes are used for high priority traffic and "worse" codes have been used for best effort. See annex E for added literature on the subject. At this time this work is fairly in the world of academia and involves fairly complex algorithms but offer promises that CDMA can allow QoS to be provided for multimedia traffic.

6.3.1.6 Onboard processing

Onboard processing's impacts on QoS can be important. They include:

- a potential reduced delay for bandwidth allocation if allocation is performed onboard;
- the possibility to queue SDUs by traffic class and apply traffic shaping onboard (at the expense of added queuing delay);
- the potential of using MPLS-like routing from uplink to downlink (see clause 7.5.5.1); and
- a better coordination between ground and space segments for admission/flow and congestion control.

These topics will be reviewed in details in clause 7.

6.3.1.7 Intermittent accessibility

Most broadband systems today (DSL, cable modems, optical interfaces, etc.) are "always on": after an initialization period the system is ready to forward packet without delay. While this is also true for some BSM STs most BSM are based on concepts of bandwidth sharing and bandwidth on demand. This means that if a service requires bandwidth it may have to wait until bandwidth negotiations finalize, which increases delay and may lead to time-outs or packet drops.

6.3.1.8 Asymmetry

Like ADSL and cable modems, most BSMs are essentially asymmetric. A host connected to a BSM will send all outgoing traffic over a lower rate terrestrial or satellite connection. This asymmetry may have an impact on QoS and overall IP performance. In addition, the DVB-RCS standard was designed for access networks not meshed networks. The impact on QoS may be large if double satellite hops are necessary to send data to its final destination.

7 BSM IP QoS management

7.1 Functional model for BSM QoS

According to the EG 202 009-1 [9] "Quality of Service" (QoS) is defined: "as the collective effect of service performances which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as:

- service operability performance;
- service accessibility performance;
- service retainability performance;
- service integrity performance; and
- other factors specific to each service".

In Internet terms this translates into the ability to segment traffic between service types or streams in order for the network to prioritize certain services over others while treating all traffic of the same type similarly. QoS encompasses both the service categorization and the overall performance of the network for each category.

The Internet Engineering Task Force (IETF) work on providing QoS over IP resulted in the development of 2 different models starting in the mid-1990s: Integrated services (Intserv) in 1994 and Differentiated services (Diffserv) in 1998.

A functional model for the implementation of BSM QoS is presented in figure 8 [12]. As was seen in the previous clause, the C-plane functions establish the BSM bearer services in response to user demands. These include signalling reservation and bandwidth allocation. The U-plane functions access individual packets for marking, classification and drop. These functions operate above and below the SI/SAP interface.

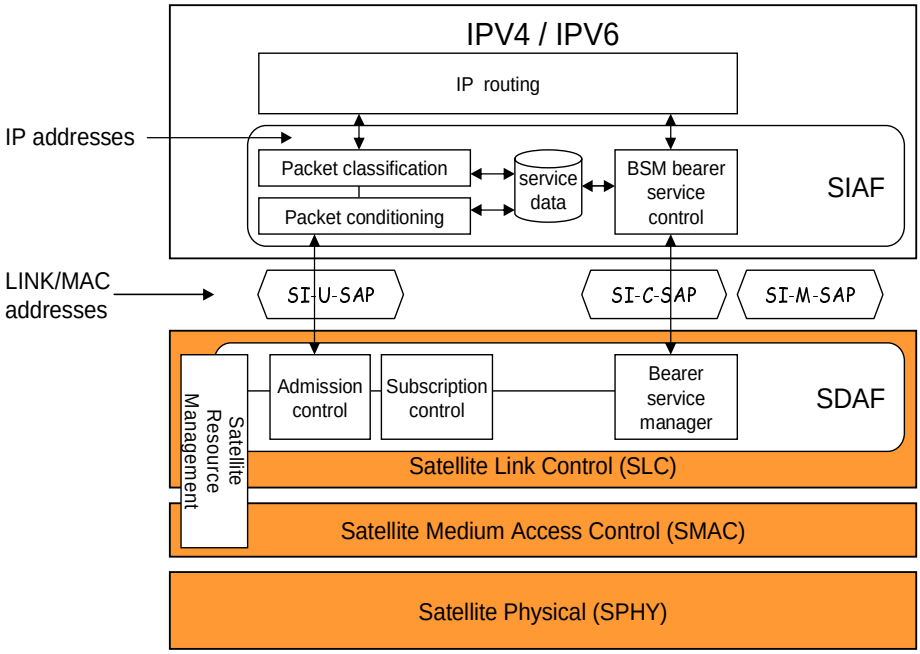


Figure 8: QoS functional model [12]

In addition, the BSM can interoperate at different layers in the OSI stack which has different impacts on QoS. The functions of the BSM include:

- bridge - below the IP layer at the frame level - the BSM as "Ethernet";
- IWU - IP interworking unit at the IP layer - the BSM as "router"; and
- Gateway - above the IP layer - the BSM as "resource manager".

In the present document, QoS will be addressed at every level and it will describe how standard methods are impacted by BSM operations.

7.2 Traffic and QoS classes

In order to deploy QoS management, traffic classes are defined and their management parameters are negotiated between providers. The use cases and services can help define these classes. This clause presents the traffic classes defined by a number of standardization groups that relate to BSMs. The traffic classes are intended to be the basis of agreements between end-users and network service providers, and between service providers. These classes are going to be used in clause 9 to define performance targets associated with each class.

QoS management in the BSM inherits from work previously done in the wireless world and in other ETSI standardization groups. This clause briefly describes some major inputs from these groups. So while the BSM does not have a set of specific traffic class it could use either of the presented approaches or define a specific one (see clause 10 on recommended TSs).

7.2.1 ITU-T

Table 4 presents a set of QoS classes defined in the ITU-T Recommendation Y.1541 [27]. ITU-T Recommendation Y.1541 applies to international end-to-end IP network paths. It defines 6 classes with 4 node mechanisms. The advantage of this classification is the provision of a special signalling class that is needed for time sensitive QoS management. However this classification does not provide for distinguishing between fixed packet size (like voice) and variable packet size (data and video) applications. This property could be used to better specify required network resources.

Table 4: Guidance for IP QoS classes from the ITU-T Recommendation Y.1541 [27]

QoS Class	Applications (Examples)	Node Mechanisms	Network Techniques
0	Real-Time, Jitter sensitive, high interaction(VoIP, VTC)	Separate Queue with preferential servicing, Traffic grooming	Constrained Routing and Distance
1	Real-Time, Jitter sensitive, interactive (VoIP, VTC).		Less constrained Routing and Distances
2	Transaction Data, Highly Interactive, (Signalling)	Separate Queue, Drop priority	Constrained Routing and Distance
3	Transaction Data, Interactive		Less constrained Routing and Distances
4	Low Loss Only (Short Transactions, Bulk Data, Video Streaming)	Long Queue, Drop priority	Any route/path
5	Traditional Applications of Default IP Networks	Separate Queue (lowest priority)	Any route/path

7.2.2 TIPHON

ETSI Project TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) is dedicated to telephony but offers heritage to the BSM QoS. It allows network operators and service providers, to offer those telephony services over multi-protocol packet-and circuit-switched networks, the BSM being one of them. However for the BSM it is necessary to look beyond the voice protocols. BSM services have to be offered in a coherent way between multiple service providers and in scenarios where the BSM interfaces with multiple technologies. TIPHON has dedicated a lot of effort to QoS that can be taken as a basis for some of the BSM work. Table 5 lists the traffic classes defined for TIPHON.

Table 5: Traffic classes from TIPHON [15]

Class	Components	General QoS characteristics
Real-time conversational (e.g. telephony, teleconference, videophony and videoconference)	Speech Audio Video Multimedia	Delay sensitive Delay variation sensitive Limited tolerance to loss/errors (depends on coding) Constant Bit Rate or and Variable Bit Rate
Real-time streaming (e.g. audio and video broadcast, surveillance, graphics)	Audio Video Multimedia	Tolerant to delay (buffering in terminals) Delay variation sensitive (depending on buffer sizes in terminals/gateways) Limited tolerance to loss/errors (depends on coding) Variable Bit Rate
Near real-time interactive (e.g. web browsing)	Data	Delay sensitive (interactive services) Tolerant to delay variation Error sensitive Variable Bit Rate
Non real-time background (e.g. email and file transfer)	Data	Not delay and delay variation sensitive Error sensitive Best Effort

In addition TIPHON defines three classes of end-to-end speech QoS [15]:

- WIDEBAND: This is a type of IP telephony service will provide a user experience better than the PSTN. It is expected that these systems will be implemented using wideband codecs and QoS-engineered IP networks;

- NARROWBAND: This is a type of IP telephony service will provide a user experience similar to PSTN. It is expected that such systems would also be implemented over QoS-engineered IP networks:
  - NARROWBAND/HIGH: This quality is equivalent to recent ISDN services;
  - NARROWBAND/MEDIUM: This quality is equivalent to recent wireless mobile telephony services in good radio conditions;
  - NARROWBAND/ACCEPTABLE: This quality is equivalent to common wireless mobile telephony services.
- BEST EFFORT: This type of service will provide a usable communications service but will not provide guarantees of performance.

The TIPHON speech QoS classes WIDEBAND and NARROWBAND have a performance guarantees for 95 % of all connections.

While this is not fully applicable to the larger band and connectionless IP services over the BSM, the TIPHON classes will influence both the BSM QoS classes and performance goals. When appropriate the TIPHON heritage the BSM can build on is highlighted throughout the present document.

7.2.3 3GPP/UMTS/GPRS

Like for TIPHON the next generation cellular and mobile packet service consider an end-to-end QoS. This results in a number of specific requirements [2]:

- QoS attributes (or mapping of them) should not be restricted to one or few external QoS control mechanisms but the QoS concept should be capable of providing different levels of QoS by using UMTS specific control mechanisms (not related to QoS mechanisms in the external networks);
- all attributes have to have unambiguous meaning;
- QoS mechanisms have to allow efficient use of radio capacity;
- they must allow independent evolution of Core and Access networks as well as cellular networks;
- applications should be able to set QoS values for their data transmissions; and
- QoS behaviour should be dynamic, i.e. it shall be possible to modify QoS attributes during an active session.

In order to do this a set of traffic classes (table 6) and QoS characteristics (table 7) have been developed. They relate to the ITU-T classes of table 4 where the ITU classes 0 and 1 map into the conversational classes, the ITU class 3 and (some) 4 map to the streaming class, class 4 also applies the interactive class. Background is obviously ITU class 5.

Table 6: Traffic classes from 3GPP/UMTS [2]

Traffic class	Intended usage	Example applications
Conversational	Real-time conversational traffic involving conversing entities	telephony, teleconference, videophony and videoconference, chatting, net-gaming
Streaming	Real-time streaming traffic involving the sending of information from one entity to another	audio and video broadcast, surveillance
Interactive	Near real-time interactive traffic involving retrieving of information by one entity, from another entity	web browsing
Background	Non real-time background traffic involving the sending of information from one entity to another entity	Email and file transfer

Table 7: Traffic characteristics from 3GPP/UMTS

Traffic class	Components	General traffic characteristics
Conversational	Speech Audio Video Data MM	Constant Rate (CR) and Variable Rate (VR) Delay sensitive Delay variation sensitive Limited tolerance to loss/errors (depends on coding)
Streaming	Audio Video MM	Variable Rate (VR) Tolerant to delay (buffering in terminals) Delay variation sensitive (depending on buffer sizes in terminals/gateways) Limited tolerance to loss/errors (depends on coding)
Interactive	Data	Variable Rate (VR) Delay sensitive (but more tolerant than conversational) Tolerant to delay variation Loss/error sensitive
Background	Data	Best Effort (BE) Not delay sensitive Tolerant to delay variation (and more tolerant than interactive class) Loss/error sensitive
NOTE: Adapted from 3GPP.		

7.3 Layer 2 QoS management

This clause introduces how some QoS management can be provided at the layer 2 of the OSI model. While not really network level QoS, this is especially applicable over the BSMs that provide bridging. A number of layer 2 mechanisms for BSM are also introduced.

7.3.1 Ethernet priorities

Ethernet priorities are currently used in virtual LANS (VLANs) and Ethernet over MPLS in Metropolitan Networks. In traditional Ethernet, the Medium Access Control (MAC) protocol is used to provide the data link layer of the Ethernet LAN system. The MAC protocol encapsulates payload data by adding a 14 byte header before the data and appending a 4-byte (32-bit) Cyclic Redundancy code (CRC) after the data. The entire frame is preceded by a 7-byte preamble and a byte of start of frame.

The 802.1p is an extension of the 802.1D (bridging standard) [21]. It specifies how prioritization can be added to the MAC layer bridge; regardless of the underlying media this adds priorities to Ethernet. The priority bits are shown in the 802.1q frame (figure 9) with an additional 4 bytes of header for the added information for Virtual LANs (VLANs) etc. With 802.1p switching capabilities, the implementation of services with 8 levels of priority is enabled end-to-end across an Ethernet network.

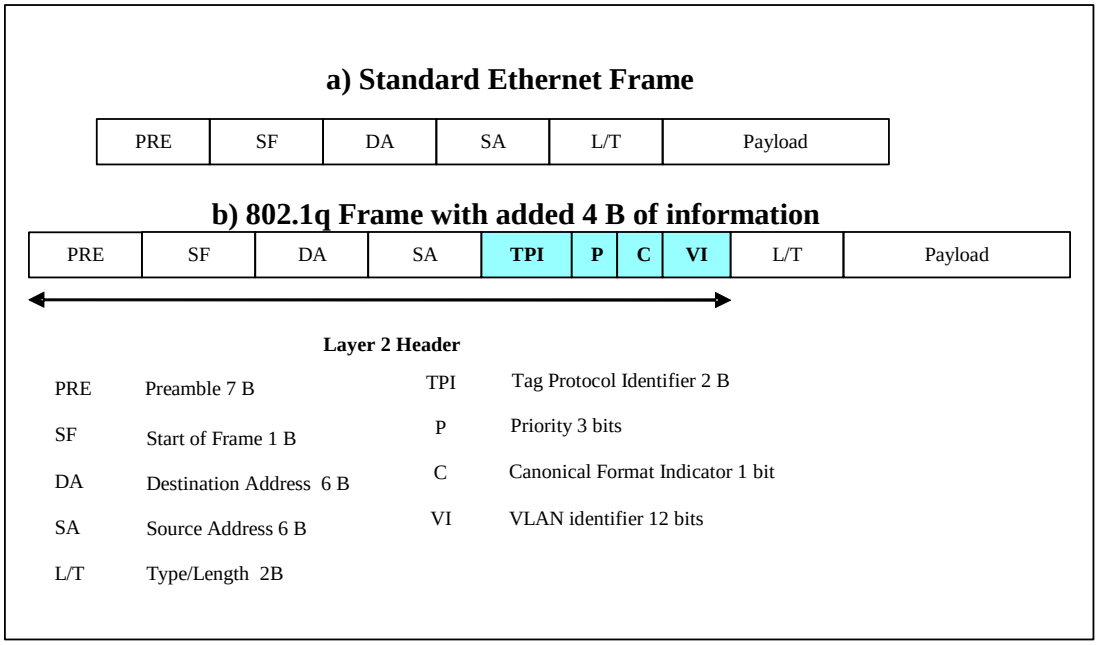


Figure 9: Ethernet 802.1q framing

7.3.2 BSM Layer 2 mechanisms

A Layer 2 (bridge) network is used to interconnect LAN segments. It only forwards valid (i.e. error checked) frames and usually provide filtering of frames based on their source addresses (SA) or other MAC addresses. As was mentioned in the previous clause, the BSM connectivity includes bridging. This clause investigates which Layer 2 BSM mechanisms can enhance the BSM QoS.

7.3.2.1 MAC Layer mechanisms

These mechanisms are implemented at the frame level and concern mainly the connectivity functions of the BSM.

7.3.2.1.1 Ethernet priority mapping to BSM priorities

If a BSM is used to interconnect LANs or Virtual LAN (VLAN) using extensions to the Ethernet protocol, then only frame interworking is necessary. The external frames, for example Ethernet are terminated in the ST and either the L2 payload or the IP payload is recovered, segmented and encapsulated into the BSM PDU. The relatively small number of Ethernet priorities (8) makes it easier to map on BSM native priority schemes

7.3.2.1.2 Point to Point IP over Ethernet and over ATM

Point to Point IP over Ethernet (PPPoE) and Point to Point IP over ATM (PPPoA) are widely used over the terrestrial ADSL network. In that case the BSM acts as a true bridge for Ethernet and as a "wire" for ATM. All QoS management is provided above IP. The BSM connection is thus transparent to PPPoE/PPPoA and transports frames directly.

7.3.2.2 Bandwidth on Demand (BoD)

There is a large body of publications on the topic of "Bandwidth on Demand" (BoD). BoD defines a bandwidth sharing mechanism that allocates bandwidth to requesting session based on a number of parameters including priorities and other QoS-related mechanisms. BSM with BoD got started as LAN interconnection via Satellite using Very Small Aperture Terminals (VSATs). BoD is mainly thought of as a return link mechanism, but even in a star configuration it can be used on the forward link to generate traffic from a destination ST. Obviously in a mesh network it can be used both on the forward and return links.

BoD has profited from the developments on ATM via satellite [66] and the DVB-RCS standardization [8]. Signalling for bandwidth is made either inside the satellite cell stream and/or using dedicated channels. BoD is also usually closely related to the satellite transmission scheme (TDMA or MF-TDMA) and can be used in conjunction with contention based signalling. One major challenge of the BoD methods is how they relate to the higher layer QoS mechanisms (like RSVP - see clause 7.5.1.1).

7.3.2.3 Link Layer mechanisms

Since the radio spectrum and geostationary orbit slots for new satellites are limited resources it is important to investigate means to improve these resources in order for the BSM to get more bandwidth to allocate to services that provide QoS and hence added revenues. Link layer methods are almost universally used independently of other mechanisms to maintain the link budget. However they impact admission/congestion/flow control because they can generate more bandwidth that can then be allocated to sessions. In order of complexity they include:

- power control;
- variable FEC;
- variable information/symbol rate; and
- variable modulation.

7.3.2.3.1 Power control

Power control uses the variability in transmission conditions (weather in particular) to vary the transmission power of a terminal to maintain the link budget. Its principle is simple: use lower power in good weather, increase power when weather goes bad. Uplink power control is widely used and part of many terminal design. On some regenerative satellite power control can also be used on the downlink but its complexity (use of narrow beams, terminal specific information) may prevent this.

7.3.2.3.2 Use of FEC

In the BSM the channel error correction allows the upper layers to receive what is essentially error-free data. Because of FEC, on the link, the "detected" errors will either lead to correction and delivery or rejection and packet loss/retransmission. The second case results in added delay and potential loss hence a QoS impact but will not be received at the IP Layer hence in principle not get accounted for but may result in retransmission hence delay that will lead to loss. "Undetected" link errors will lead to an errored packet being delivered by the BSM see (clause 8.4.3.2.3). These errors may be found by the CRC and will also be dropped leading directly to packet loss. In fact the total loss should be the sum of both contributions but requires monitoring at 2 layers.

While "static" FEC, where the ratio of information to symbols remains constant has proven extremely valuable, variable FEC is now widely considered for advanced BSMs. Varying the coding rate is similar to power control but at the symbol level. In times of bad weather or other low signal to noise ratio a lower rate FEC code can be used to maintain the higher layer error free, hence maintain the packet loss (and the QoS) at the specified level. With the use of rate compatible codes, the symbol rate can be kept constant but the number of information bits per frame is reduced. This reduces the size of the "pipe" that was sold to users. The use variable rates must be coordinated with the management and traffic policies at the higher layers to ensure that traffic and QoS guarantees are maintained and that only best effort (or low priority traffic) is impacted by a change in the information rate. The impact of these techniques on the complexity of the transmission systems is beyond the scope of this note.

7.3.2.3.3 Variable information/symbol rate

Another way to improve the link budget is to reduce the rate transmitted by the ST. By doing that the link budget improves by a number of dBs. As was mentioned above, the service can continue either with degraded performance for all services (if the service agreements allow it) or at nominal performance for high QoS classes by shutting down some low priority services.

7.3.2.3.4 Variable modulation

It is well known that the spectral efficiency of satellite networks can be increased through the use of higher level modulations such as 8-PSK and 16-QAM as compared to traditional QPSK modulation. The new high powered satellite transponders combined with concatenated error correction techniques allow the use of these higher modulation techniques. The downside of these techniques however is that while the use of higher level modulation techniques improves the bandwidth efficiency for a given $E_bN_{0,}$ it is at the cost of more transmitter power or higher earth station G/T and greater earth station e.i.r.p. hence higher cost ST. The ITU-R Recommendation S.1425 [24] establishes the requirements for the amplifiers that need to be used to support higher-level modulation.

7.4 ATM

The Broadband Integrated Service Digital Network (B-ISDN) was developed to become an all purpose network technology to provide multimedia services. While it has failed as a desktop technology it is still widely deployed in the core networks. The Asynchronous Transfer Mode (ATM) was proposed as the B-ISDN transport. While ATM was originally and is still mostly used over fibre networks there has been considerable work on ATM over wireless and satellite networks. While ATM is not the focus of this note it is important to review some of its concepts because of its influence on IP QoS.

7.4.1 ATM QoS management

ATM provides four main classes of service, Continuous Bit Rate (CBR) or Deterministic Bit Rate (DBR), Variable Bit Rate (VBR), Available Bit Rate (ABR) and Unspecified Bit Rate (UBR). The first three have traffic descriptors that allow allocating resources to requesting calls. CBR traffic is characterized by a Peak Cell Rate (PCR) in essence the bandwidth of the connection. VBR traffic allows for statistical multiplexing and uses the PCR and two other parameters: the SCR, the sustainable cell rate or the average bandwidth required to maintain the service and the Mean Burst Size (MBS) that is used to manage sudden bursts of traffic. ABR traffic uses the PCR and a minimum cell rate or minimum rate need to maintain the service. ABR services have to delay guarantee as VBR and PCR do. All sources are policed at the User Network Interface (UNI) [4].

ATM is essentially connection oriented. It uses concepts of virtual connections to switch short 53 byte cells (5 bytes header and 48 bytes payload) in the ATM cloud. There is heritage in supporting IP over ATM that has influenced how other technologies transport IP packets.

7.4.2 ATM via satellite

For BSMs the most important ATM concepts are described in the User Network Interface (UNI) [4] that has influenced the design of the BSM SDUs and satellite payloads (ATM-like). In particular, the focus of satellite ATM was put on how to provide the ATM classes of service efficiently. In view of the fact that the BSM uses a shared medium, not native to ATM, a new MAC was needed in addition to the work done on onboard switching and queuing using ATM concepts [66].

7.5 Layer 3 IP QoS management

In the past decade IP networks have moved from providing a single best-effort service to multiple types of services with QoS, generally bounded packet delay and loss. Although the majority of the network traffic presently is still best-effort, emerging networked applications with different QoS constraints found in typical multimedia applications are becoming prevalent, and may soon contribute appreciable share of total network traffic. In addition, users are demanding better QoS guarantees for their traffic, or QoS differentiation for their Virtual Private Networks (VPNs).

The support for Internet QoS seems to evolve into 2 main models:

- a call-based model combining SIP signalling, explicit resource reservations with RSVP and synchronization using COPS; and
- an aggregate model combining label-switching to control paths and packet markings within domains.

This clause introduces the main elements of each of these models for QoS management at the network layer and how they impact or are impacted by BSM networks.

7.5.1 Integrated services: the Intserv model

The Integrated Services (Intserv) model was developed to support real time applications and guaranteed resources over the IP protocol. Intserv is flow-based hence deals with a series of datagrams from a single source to a single destination that share a common set of quality of service parameter such as bandwidth, delay, etc.

Intserv provides fine-grained service guarantees to individual packet flows in terms of guaranteed and controlled services beyond the usual best effort. It is described in the RFC 1633 [34]. An IP flow is identified by a flow specification (flowspec). This creates stateful associations between individual packets by matching fields in the packet header. Bandwidth is reserved for the flow, and appropriate traffic policies are implemented on every router in the path from source to destination. Because Intserv requires installation of state information in every participating router guarantees are not enforced unless all routers have been reached by the reservations and have successfully recorded the appropriate "state".

Intserv defines three levels of service, one being Best Effort (BE), in fact the absence of QoS. The two others are Guaranteed Services and Controlled Load Services. Guaranteed Service (GS) defined in RFC 2212 [41] offers hard upper bounds on delay to flows that conform to a traffic specification (TSpec). By using a fluid flow model the TSpec is related to the reserved bandwidth (RSpec) and to variable delay. IP packets sent above the RSpec (non-conforming) packets are considered as best effort and could be discarded. The Controlled Load Service (CLS) defined in RFC 2211 [40] offers low delay and packet loss to flows that conform to a TSpec, but no hard bounds as compared to GS. Again non-conforming packet are considered BE.

Table 8: RSVP messages

RSVP message name	RSVP message function
PATH	The PATH Message is sent by a source that initiates the communication session. It explicitly bids the data path of a flow. It also describes the capabilities of the source.
RESV	The RESV message is issued by the receiver of the communication session and it follows exactly the path that the RSVP PATH message has followed hop by hop back to the communication session source. The RESV message in its way back to the source may install QoS states at each hop. These states are associated with the specific QoS resource requirements of the destination. The RSVP reservation states are soft states that have to be updated regularly.
PATH Error	Used to report errors that occurred during the installation of a path from the source to the destination of a communication session.
RESV Error	Used to report errors that occurred during the installation of a reservation state along the communication session path.
RESV Confirm	It provides a positive indication to the initiator of the communication session informing that all nodes along the communication session path accepted the reservation request. The RSVP confirmation messages are typically sent by the source of the communication session directly to the destination of this communication session. Intermediate nodes do not process RSVP confirmation messages.
PATH Tear	Sent by the source of the communication session and explicitly deletes the stored QoS path information on all nodes included in a communication session path.
RESV Tear	Sent by the destination of the communication session and explicitly deletes the stored QoS state information on all nodes included in a communication session path.

Using RSVP, the currently accepted method (but not the only one) (RFCs 2205 [38] and 2210 [39] see below) bandwidth is reserved for the flow. RSVP also specifies the parameters that will enable traffic conditioning and packet scheduling in all routers along the path.

Intserv and stateful reservation protocols such as RSVP have failed to become the end-to-end QoS model of choice. This is because of the need to support the model in all network devices from source to destination. In addition Intserv and RSVP need a lot of processing at each node keep state information and require usage-based accounting, to account for conforming and non conforming packets. This results in reliability and scalability issues in the core network but also makes Intserv too heavyweight for small terminals especially mobiles. It is however proposed and supported in smaller networks and at the edge.

7.5.1.1 Resource ReSerVation Protocol (RSVP)

RSVP- described in RFCs 2205 [38] and 2210 [39] is a signalling protocol designed to request a specific Quality of Service (QoS) from the network for a data stream. While not strictly at layer 3 (slightly above) it influences the work of routers and other network elements.

An RSVP request is propagated node to node through the network through the nodes the data would be routed through. At each node, the resource reservation is made by invoking local admission and policy control. If both accept the request, the reservation information is used to set parameters in the local packet classifier (to determine a packet traffic class) and scheduler to provide the requested QoS. If the request cannot be accommodated, an error message is returned to the request originator.

RSVP does not specify a routing protocol. It uses the current routing protocol decisions to determine where the requests should be sent. As such it is compatible with both variable and fixed path routing algorithms and has been extended to MPLS and other new algorithms to provide traffic engineering mechanism and carry policy control messages. It is compatible with both multicast and unicast routing. It also provides for authentication: in order to accept a RESV message a mechanism may need identification of the user of the RESV message (i.e. one with whom it has some peering agreement). Finally, RSVP runs over both IPv4 and IPv6. Table 8 summarizes the RSVP messages.

Table 9: Flowspec Example: TSpec and RSpec for VoIP (RTP), G.711 codec @ 20 ms framing

Parameter	Value
Bit rate/Byte rate	64 kbps nominal bit rate = 8 kBps nominal byte rate
Framing rate	20 ms or 50 packets/sec There could also be the specification of a "slack term" to control delay and jitter bounds.
Payload size	8 kBps/50 packets ;160 bytes per packet of payload
Packet size	Add 42 bytes of IP/UDP/RTP header 202 bytes per packet/10 100 bytes/s byte rate
Sender and Reverse Sender TSpec	
Bucket Depth (b) bytes = VoIP datagram size, including IP/UDP/RTP header overhead	202 bytes
Bucket Rate (r) bytes/s = actual data rate, including IP/UDP/RTP header overhead	10 100 bytes/sec
Maximum Datagram Size (M)	202 bytes
Minimum Policed Unit (m) bytes	202 bytes
Sender and Reverse Sender RSpec	
Reserved Rate (R) bytes/s	10 100 bytes/sec

7.5.1.1.1 RSVP QoS parameters

A RSVP reservation defined in RFC 2205 [38] request consists of two parts: a "flowspec" and a "filter spec". Together they form a "flow descriptor". The flowspec specifies the desired QoS. The filter spec, together with a session specification, defines the "flow" (in data packets) to receive the QoS defined by the flowspec. The flowspec is used to set parameters in packet schedulers or other link layer mechanism. The filter spec is used to set parameters in the packet classifier. Data packets that are addressed to a particular session but do not match any of the filter specs for that session are handled as best-effort traffic. The flowspec in a reservation request generally includes a service class, an "Rspec" (R for "reserve") that specifies the desired QoS, and a "TSpec" (T for "traffic") that specify the data flow. Rspec is used for guaranteed reservations, in terms of delay and rate. Tspec is used for classification and may be used for traffic shaping (see clause 8.2.3) if the router performs policing and shaping. Consequently, every RSVP flowspec will contain a Tspec but only messages that guarantee bandwidth and delay will contain an Rspec. The formats and contents of Tspecs and Rspecs are determined by the Intserv model (see RFC 2210 [39]). An example of a flowspec is available in table 9.

7.5.1.1.2 Support to multicast

RSVP already supports multicast but it has not been widely deployed in multicast networks.

7.5.1.2 Session Initiation Protocol (SIP)

SIP is defined in RFC 3261 [63]. Originally defined for Voice over IP (as a replacement for the H.323 protocol) it is now extended to multimedia conferencing, messaging etc. SIP initiates multi-media sessions between two or more users and as such is a higher layer signalling protocol.

SIP provides [67]:

- registration;
- session set-up (finding the other party/parties);
- session control (changing call characteristics); and
- session termination (closing the session).

By itself, SIP does not provide services. Rather, SIP provides primitives that can be used to implement different services. Since SIP messages and the sessions they establish can pass through entirely different networks, SIP cannot, and does not, provide any kind of network resource reservation capabilities but relies on other protocols to do so.

In addition, SIP is a high layer component that can be used with other IETF protocols to build complete transmission architectures. These include Real-time Transport Protocol (RTP) for real-time data and providing QoS feedback, the Real-Time Streaming Protocol (RTSP) for controlling the delivery of streaming media, the MEdia GAteway COntrol protocol (MEGACO) for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP) for describing multimedia sessions. In addition, it is generally accepted that SIP relies on RSVP to reserve the resources necessary to transport the SIP session end-to-end. But SIP can also and will work over best effort networks and Diffserv transit networks (see clause 7.5.2) as the latter can have class specifics for signalling and multimedia.

The basic SIP client server model and messages to establish, confirm and leave sessions (known as "methods") are available in figure 10. In addition figure 11 shows a typical SIP request. For QoS it is the SDP message that has importance, in particular the qos-attribute. If the qos-attribute is set, it requests QoS services and it will trigger the appropriate resource reservation mechanisms (table 10).

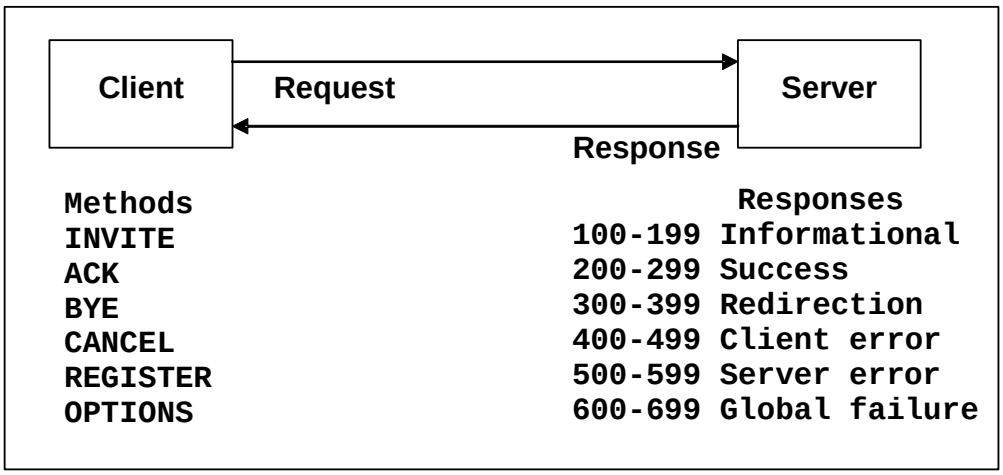


Figure 10: SIP Client Server Model [67]

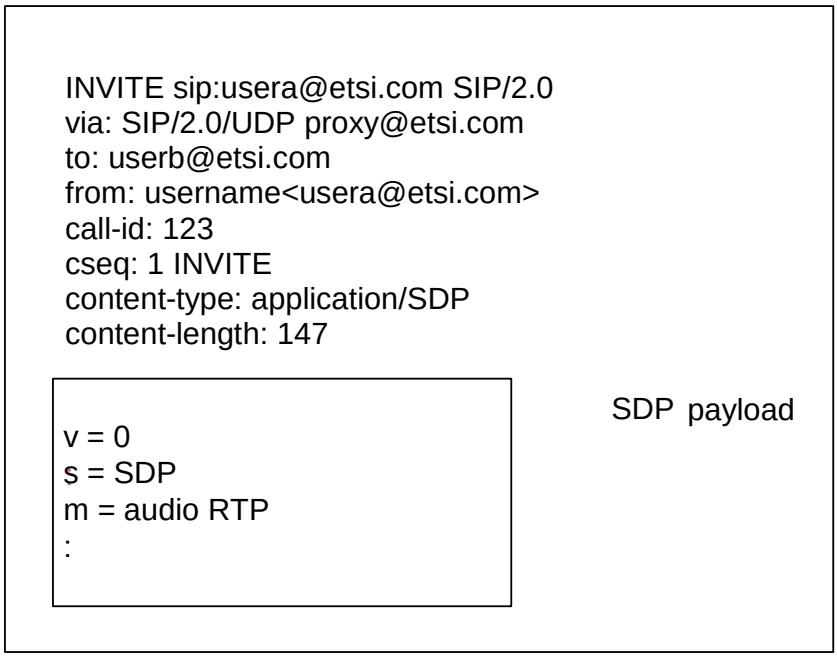


Figure 11: SIP syntax [67]

Table 10: SIP QoS mechanisms

SIP call setup	Result
Bandwidth reservation (QoS) is attempted when:	The desired (requested) QoS for the associated peer in the SDP message is set to qos-assured|qos-enabled qos-attribute = qos-assured|qos-enabled need a definition if this is controlled-load or guaranteed-delay
Bandwidth reservation (QoS) is not attempted when:	The desired QoS level is set to the default of best-effort. qos-attribute = or qos-attribute = best-effort Or the qos-attribute is not set.

7.5.1.3 Interaction with COPS

The Common Open Policy Service (COPS) is a policy based authorization and provisioning protocol [59]. The COPS protocol is used to transmit policy from a Policy Decision Point (PDP) to a Policy Enforcement Point (PEP). In particular COPS can implement simple client/server architectures for supporting policy control over QoS signalling protocols. The base protocol can be but is not limited to RSVP. The COPS model does not make any assumptions about the methods of the policy server, but is based on the server returning decisions to policy requests so it can be extended to a number of operators' management policies. In the service provider world, where QoS is not free, COPS can also be used to provide support for billing and authorization via the SLA.

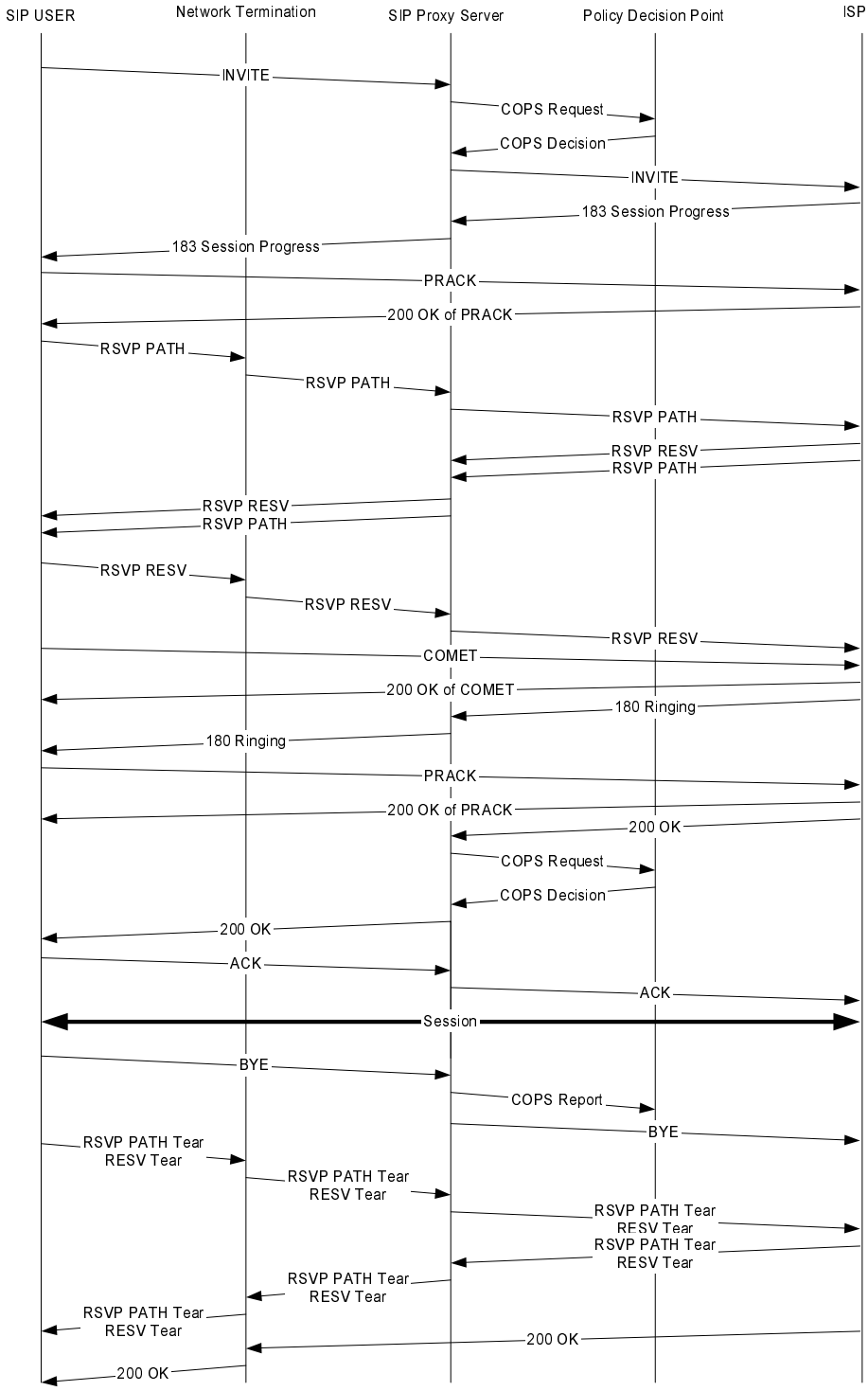


Figure 12: Interaction of SIP, COPS and RSVP

Figure 12 shows the interaction between SIP, COPS and RSVP over a terrestrial network. An INVITE message containing QoS requirements and resource reservation is sent to the destination. At the SIP proxy this message triggers a COPS interaction that contains the information from the SIP message, to authorize and admit the session and enable QoS policy servers. After receiving a positive acknowledgement the INVITE message is sent to the destination's ISP. The 183 session progress is sent while the SIP QoS conditions are processed. This triggers a processing acknowledgement sequence (PRACK and 200 PRACK) while the QoS reservations are under way. The RSVP PATH and RESV messages (bi-directional) are used to reserve the resources necessary for the session. The COMET message signals the reservation was successful and is followed by a 180 ring message that in this case requires reliability check hence the PRACK sequence. Finally the data can flow. At the end of the session a shorter sequence breaks the connection.

7.5.1.4 Use of RSVP/Intserv over BSM

For RSVP, the BSM offers an advantage over terrestrial wired networks: because of the coverage of most BSM there will be a lesser number of routers on the reservation path of the BSM than on the equivalent terrestrial network. This helps alleviate some of the scalability issues of RSVP. Intserv (and RSVP) in the BSM world can create the mechanism to ensure the user of the resources is known. However, since RSVP is stateful, on a RSM, it may require keeping states onboard, a reliability issue.

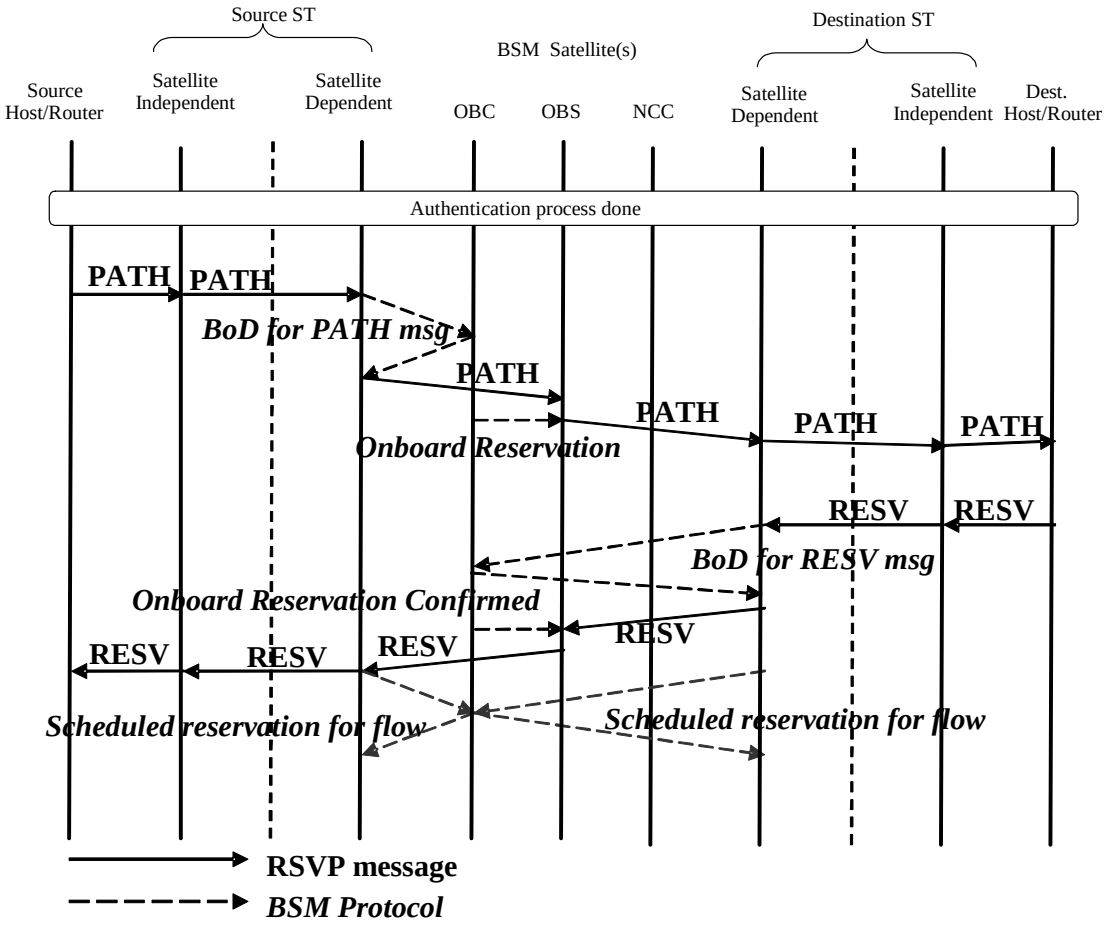


Figure 13: RSVP over a BSM with onboard switching (one way reservation)

In RSVP, at the SI interface flowspec parameters need to be translated into satellite units and in particular bandwidth requirements. There is a close coupling between what RSVP needs and what Bandwidth on demand can provide. Hence RSVP leads to scheduled requests for bandwidth to ensure that the reservation is met when the traffic flow traverses the BSM. Flowspec will also set queuing parameters and traffic shaping in the ST transmission queues. The ST however cannot end the messages; they have to be processed locally and sent downstream as requested by the protocol.

Figure 13 shows an example of RSVP over a RSM type BSM (in a transparent system the onboard operations would be done in a gateway or NCC). In this figure the onboard processor is separated into a OBC, the controller, and the OBS, the switch. At the IP layer, the BSM processes the RSVP message like a usual router. The response to the request however involves the BSM to perform bandwidth on demand to transport the PATH and RESV messages, include an onboard reservation to support the reservation onboard pending the reply of other routers on the path. Once the RESV message returns, the ST establishes a scheduled or permanent uplink bandwidth reservation to support the RSVP flow with the accepted bandwidth and delay. This is just an example but it illustrates that the use of RSVP can be accommodated within the BSM by the appropriate mechanisms.

As illustrated by the previous example, RSVP (over the BSM) signals requests and periodically refreshes them. Some mechanisms must be provided to make sure there is bandwidth for that signalling and that the delay for allocating the bandwidth does not create timeouts. Pre-emption classes have been proposed to do this [62]. For the BSM, a packet marked "pre-emption" would have the capability of taking the place of another scheduled packet, hence possibly leading to a temporary reduced performance for another class; this goes beyond a precedence class. Obviously very little traffic would be marked "pre-empt" and overall performance would not suffer. The pre-emption class would only be used for traffic that needs to go through for overall network performance to be maintained.

Over the BSM, the combination of SIP/COPS and RSVP can lead to long delays as shown in figure 12. In this context multiple satellite hops should be avoided. However COPS will be an important protocol to allow interaction between the BSM QoS management located in the NCC and an external (to the BSM) SIP proxy. In an end-to-end view, multimedia QoS negotiation can be invoked by SIP to define a QoS path via a series of intermediate SIP servers. This is well above the BSM but as was seen in clause 7.5.1.2 that the SIP QoS settings mostly use the Intserv model and RSVP. The BSM may participate in the QoS setup via a COPS dialog between the BSM proxy (middleware) and a local SIP server (also possibly owned by the satellite operator or service provider), taking the role of the Policy Decision Point in figure 12.

Finally, some BSMs use path asymmetry where the forward and return channels use different sets of routers. In that case RSVP can be separated into two distinct unidirectional flows. There will be a need for defining a flowspec for each direction of a session; in fact a lot of RSVP implementations there will be reservations on both directions to ensure bandwidth is available end-to-end.

7.5.2 Differentiated services: the Diffserv model

Even with Intserv models, QoS traffic is continuing to stress existing networks, which in turn are unable to provide per-flow QoS because of scalability concerns. An answer to the above challenges is the Differentiated Service (DiffServ) (RFC 2475 [45]) framework, which delivers a coarse level of QoS in a per-node, per- class basis such that scalability is preserved. The aim of Diffserv is to provide QoS using a hierarchical approach: interdomain and intradomain. The DS framework was not intended to address end-to-end QoS issues like Intserv; it was designed to provide service providers with "better" performance goals and ones that allowed developing a customer base.

Diffserv provides coarse-grained controls to aggregates of flows. In Diffserv the QoS requirements for the customer network are aggregated and incorporated into the provider's Service Level Agreement. DiffServ mechanisms do not use per-flow signalling, and as a result, do not consume per-flow state within the routing infrastructure. Different service levels can be allocated to different groups of users, which mean that all traffic is distributed into groups or classes with different QoS parameters. At the packet level the QoS is provided by packet markings. Overall, this reduces the maintenance overhead in comparison to Integrated Services.

Diffserv does not provide any QoS guarantees, but the means to define and manage QoS guaranteed across a certain network (Diffserv domain). As such it can be made operator specific. Diffserv addresses the scaling issues of Intserv by becoming stateless except at the edge of a domain. It is only at the edge (and not at every point) that packets are classified into flows, and these flows marked, policed or shaped according to traffic conditioning specifications by a Diffserv Policy Enforcement Point (PEP). DiffServ currently only provides relative or qualitative QoS differentiation such as high bandwidth, low delay, or low loss by allocating the bandwidth to one class greater than the others, or by providing dropping preference among traffic from different classes.

7.5.2.1 Codepoints

A DiffServ CodePoint (DSCP) (figure 14), identifies Per-Hop Behaviour (PHB) and is set in each packet header. The DSCP is carried in the DS-field, using six bits of the IP header (see RFC 2474 [44]). The forwarding behaviour related to each code point is defined "locally" within each operator domain. Hence it is the role of SLAs and interdomain negotiations ensure that the right forwarding behaviour will be given to a marked packet as it moves from one domain to the next as the same DSCP may have different meaning from domain to domain. Code points do not define an end-to-end behaviour like a flow spec but more specifically how a packet will be handled in a specific domain.

The 6 bits DSCP can specify 64 Per-Hop Behaviours (PHB). The PHB denotes the forwarding behaviour to be applied to the packet in each node in the Diffserv domain. Although there is a "recommended" DSCP associated with each PHB, the mappings from DSCPs to PHBs are defined by the DS-domain. In fact, there can be several DSCPs associated with the same PHB.

The class selector PHB defined in RFC 2474 [44] offers two relative forwarding priorities:

- Expedited Forwarding (EF) PHB (see RFC 2598 [48]) guarantees that packets will have a well-defined minimum departure rate which, if not exceeded, ensures that the associated queues are short or empty. EF is intended to support services that offer tightly bounded loss, delay and delay jitter; and

- Assured Forwarding (AF) PHB group (see RFC 2597 [47]) offers different levels of forwarding assurances for packets belonging to an aggregated flow. Each AF group is independently allocated forwarding resources. Packets are marked with one of three drop precedence, such that those with the highest drop precedence are dropped with lower probability than those marked with the lowest drop precedence. DSCPs are recommended for four independent AF groups, although a DS domain can have more or fewer AF groups.

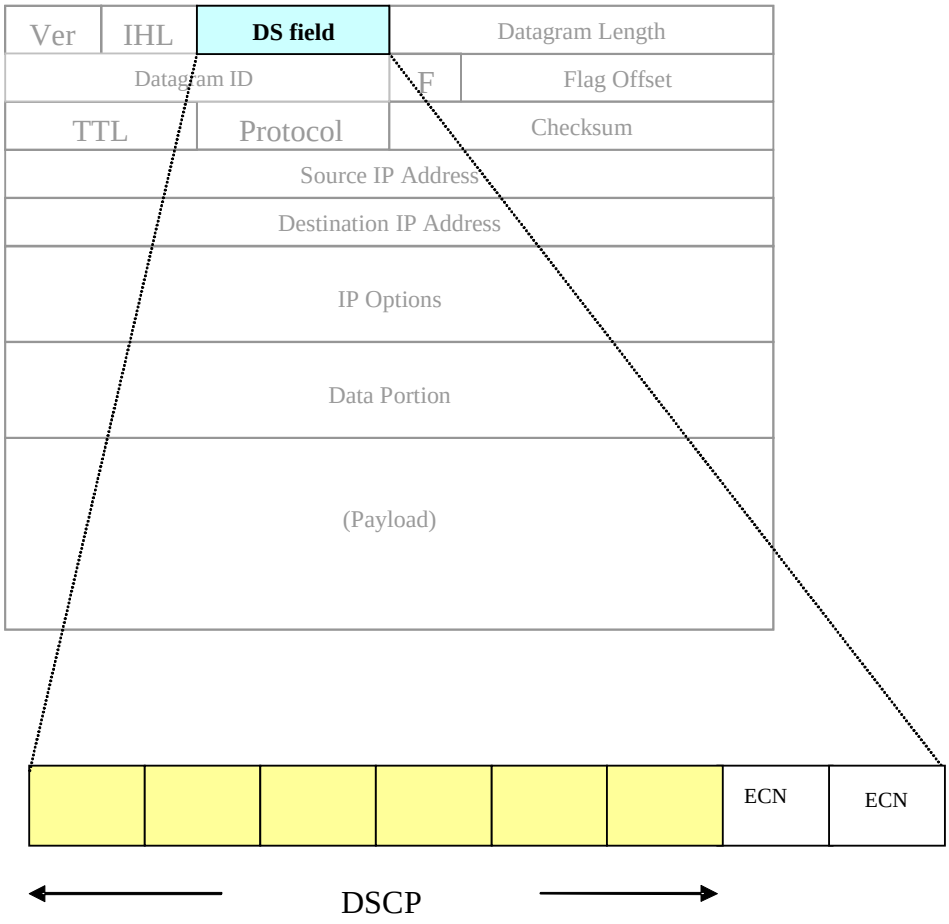


Figure 14: Differentiated Services Code Point field in IPv4 Header

7.5.2.2 Bandwidth Broker

In DiffServ, the Bandwidth Broker (BB) is an agent responsible for allocating preferred service to users as requested, and for configuring the network routers with the correct forwarding behaviour for the defined service. The idea of a BB was introduced as part of the Differentiated Services architecture to include more end-to-end aspects in DiffServ.

A BB is associated with a particular trust region, one per domain. A BB has a policy database that keeps the information on who can do what, when and a method of using that database to authenticate requesters. Only a BB can configure the leaf routers to deliver a particular service to flows, crucial for deploying a secure system.

When an allocation is desired for a particular flow, a request is sent to the BB. Requests include a service type, a target rate, a maximum burst, and the time period when service is required. The request can be made by a user or it might come from another region's BB. A BB first authenticates the credentials of the requester, and then verifies there is unallocated bandwidth sufficient to meet the request. If a request passes these tests, the available bandwidth is reduced by the requested amount and the flow specification is recorded.

The BB configures the appropriate leaf router with the information about the packet flow to be given a service at the time that the service is to commence. This configuration is "soft state" that the BB will periodically refresh.

7.5.2.3 Support to multicast

In Diffserv the packet markings and their interpretation at the end receiver and in the intermediate queues are independent of the transmission method being used. The only issue would be for users of a multicast session on different domains that could be using different semantics for the DSCP hence where packets would not be treated the same way. This however could be resolved prior to transmission amongst the provider of a high quality multicast session.

7.5.2.4 BSM support for Diffserv

The BSM architecture does not preclude the use of Diffserv at any point in the network. Actually, Diffserv is well suited for small inexpensive devices hence is not a large added cost features for small STs. DSCP can be mapped to internal BSM classes when needed. This is not an easy task as different DS domains may use a different meaning for the same DSCP. In addition, the mapping of 64 potential classes into a lesser number may not be a trivial task if the actual characteristic of each class is not known. The actual mapping may mix one-to-one and one-to-many depending on the BSM specific capabilities and queuing policies. This implies some negotiations with the networks attached to the BSM, definition of specific per hop behaviour or at the minimum an understanding of the type of traffic carried by the marked packets. DSCP mapping into the BSM is an area of interest for future work and it could become part of the satellite independent protocols. Once the DSCP is mapped into a BSM class, the SDU should carry the right information so that it is processed properly inside the BSM.

7.5.3 ITU IP transfer capabilities

As defined by the ITU, an IP transfer capability is a set of network capabilities provided by IP based networks to transfer IP packets from source to destination. This relates to the Intserv model in the sense that each IP transfer capability specifies a service model, a traffic descriptor, a traffic conformance (policy) definition and QoS requirements. The IP transfer capability is supported by appropriate traffic and congestion control that depend on the type of IP service the capability enables.

ITU-T Recommendation Y.1221 [29] defines IP transfer capabilities that relate to the IETF models, namely:

- Dedicated BandWidth (DBW) - this capability is intended to support applications with stringent delay requirements. It aims to support the guaranteed and timely delivery of IP packets along the end-to-end path of the network. It relates to the Intserv Guaranteed Services and Expedited Forwarding per hop Behaviour of Diffserv as defined in RFC 2598 [48] except that DBW expects non-conforming packets to be discarded.

- Statistical BandWidth (SBW) - supports applications, which do not have stringent delay requirements but need to have the guaranteed delivery. It relates to the Intserv Controlled Load but also to the Assured Forwarding per-hop behaviour of Diffserv RFC 2597 [47]. It can also be associated with a packet loss commitment.

- Best-Effort (BE) IP transfer capability - this is the non-QoS model where packets are not given any guarantees but will be delivered if there is enough bandwidth in the network.

7.5.4 Intserv and Diffserv co-existence in the BSM

Diffserv and RSVP models can co-exist on the same network, with Intserv deployed in the access network and Diffserv in the core network. The Diffserv/Intserv (and MPLS - see clause 7.5.5.1) combine the possibility for the hosts to request quantifiable resources along end-to-end data paths, provided by the IntServ and MPLS architecture, to the scalability provided by the DiffServ architecture.

In this model at the edges, the BSM provides QoS by being recognized as a router by the attached IP or MPLS networks while within the BSM (and the other networks) the DiffServ model is adopted. The BSM supports per-flow negotiation for Intserv and labelled path reservation established at the edge and "service" negotiation for each class supported in Diffserv (see the recommended TSs). In turn the RSVP reservations in "edge" networks are mapped by standard router mechanisms to BSM service classes by association with DSCPs.

7.5.5 QoS routing

Quality of service routing has received considerable attention in the last few years because of the emergence of services requiring QoS and the general belief that the Internet has to offer QoS to become the all-purpose network of the future.

Typically the routing decisions in the best effort Internet are at the packet level and shortest-path-based routing are the most common protocols. In addition, best effort routing is also destination oriented: the source is not taken into account when making a routing decision and the packet goes along on a hop by hop basis. QoS routing refines the IP routing problem of finding a route from source to destination by adding QoS constraints: minimum delay, fixed loss etc. Hence QoS based routing identifies efficient paths that can satisfy the given QoS constraints.

A source-destination (flow based) protocol is more appropriate to guarantee that all packets in a flow follow the same route for the duration of the flow (route pinning) and that congested nodes are avoided. This implies that the source has knowledge of the status of the network in order to make the routing decisions, something that may not be available all the time. Instead of a single path, the routers should offer alternate paths in case the network behaviour changes and the original QoS cannot be met along the chosen path and when the source does not have full knowledge of the network. This results in "crankback", the ability to reverse back to the source when a path does not meet requirements and source-link-overflow, which allows changing paths when the original path cannot accommodate a new flow.

In general routing can be separated into route determination and route execution (forwarding). Route determination can further be separated into the "protocol" (OSPF, MPLS etc.) and the "algorithm" (path search and optimization). The protocols capture the state of the network (bandwidth, resources) and disseminate it through the network. The algorithms use the information to compute paths and paths costs. In best effort networks the state of the network is fairly static. In QoS based routing the algorithms have to deal with varying states based on instantaneous information from the applications and the network. It is usually agreed that that bandwidth and delay should be used as metrics for QoS routing and as such a number of approaches have been developed.

The next clause introduces MultiProtocol Label Switching (MPLS) a layer 2.5 routing approach that prepends a label to packets before sending them on a labelled path defined according to predefined QoS requirements. MPLS has emerged recently as the routing protocol of choice to support multimedia and multi-services networks. In addition, Q-OSPF will also be discussed below.

7.5.5.1 MPLS

The Internet does not have any intrinsic connection oriented services and usually packets are more of less routed individually. This creates issues for traffic managers who would like to balance loads in the network and, for QoS, as there is not strict guarantee that all packets in a stream will follow the same path. To solve this problem, the MultiProtocol Label Switching (MPLS) Standard was developed to allow the definition of routes in the Internet in effect tunnels that have the same properties. In order to do this, MPLS adds "shim" information to the packet, between the network layer header and the layer 2 header. This is the "label" and it contains all the unique semantics that identifies the path the packet will follow. MPLS uses mechanisms to interoperate with both RSVP and IP precedence signalling. Diffserv together with MultiProtocol Label Switching (MPLS) provide a powerful and highly scalable framework for QoS provisioning in IP networks where MPLS controls the data path and DiffServ controls the QoS differentiation.

7.5.5.1.1 Routing principles

In a router, packets are sent from input port to output port based on a number of "routing" tables that contains the information mapping an input address to an output port following different rules, shortest path, lower cost etc. MPLS does not have this multiplicity: there is only one algorithm, label swapping. Operations are therefore simplified: the switch forwards ingress traffic by looking up the information in the incoming frame header, the path label and finding the egress label and port information. The payload itself is untouched. This not only allows favoured routes to be defined but allows faster processing of the packets: there are always going to be fewer paths than IP destinations for example. Only the edges of the path need to process the packet further.

7.5.5.1.2 Label definitions

The MPLS header is composed of 4 bytes of which 20 bits are label information, 3 bits are for experimental use and can be used to identify VCs at the output of a labelled path. There is 1 bit to indicate bottom of stack and a byte of Time To Live (TTL) that is used to ensure a misrouted packet gets dropped after a number of hops (figure 15).

The paths themselves are known as Label Switched Paths (LSPs) and are essentially "tunnels" where information flows from one end to another without being modified at any intermediate node. Routers that implement the MPLS protocol are known as Label Switched Routers or LSRs. Hence, the role of LSRs is to forward traffic along the a-priori defined paths in the MPLS network. The path setup enables the network operator to use proven traffic engineering mechanisms that in turn allow efficient management of network resources. In effect MPLS creates a "virtual" circuit switched network overlay above the Internet infrastructure.

LSPs must be computed and distributed in the network before any packet can be forwarded and resources (bandwidth) must be reserved for them using the Resource ReSerVation Protocol with Traffic Engineering (RSVP-TE) extensions. Hence the label information contained in the packet header suffices to route the packet from source to destination.

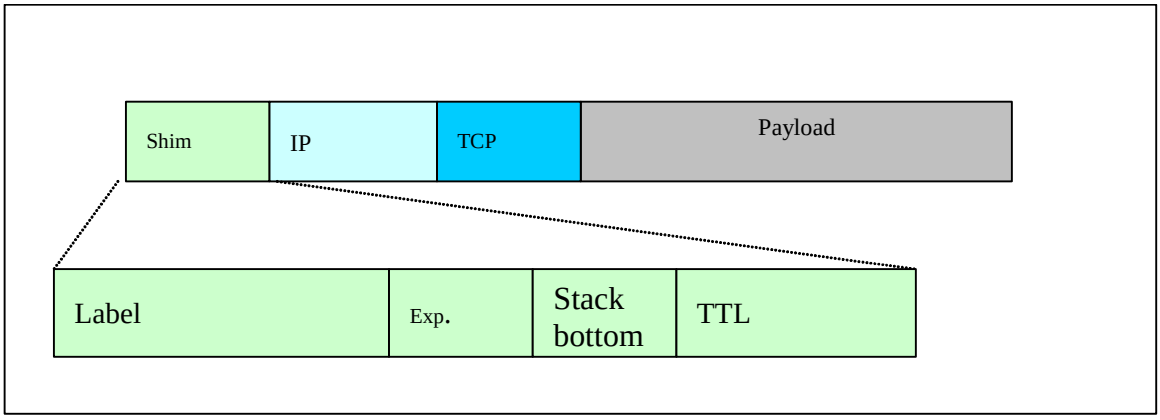


Figure 15: MPLS packet formats

7.5.5.2 Q-OSPF

Q-OSPF extend the capabilities of OSPF V2 to provide the required level of support for QoS based routing while limiting those additions to the minimum necessary set [49]. All of the existing OSPF mechanisms, data structures, advertisements, and data formats remain in place. The extensions are signalled via the Options field in OSPF Hello packets. These Options enable routers to routers to support optional capabilities, and to communicate their capability to other OSPF routers. Hence a QoS enabled router can advertise its supports QoS and find which of its peers also supports it. Q-OSPF also supports enhanced path computations and alternate routing paths based on bandwidth and delay requirements encoded in the Options and TOS headers. It is not however as deployed as other protocols as consensus on QoS routing seem to focus on sub-IP routing mechanisms such as MPLS.

7.5.5.3 BSM QoS routing requirements

Routing has been addressed in a specific TR 102 155 [13] and routing will not be discussed in details here. In the BSM where most routes are static, QoS routing becomes a queuing and traffic shaping issue. Even when dynamic routing is considered, the constraints for QoS routing over the BSM are not different than on terrestrial networks. Hence the need to recognize packet priority by marking, source/destination pairs, label etc. to route them to an appropriate route (or queue) and process them accordingly while transiting through the BSM. In addition the use of multiple routing tables indexed by QoS class can help realize QoS routing by using standard approaches. It is good practice in BSM networks to have an alternate route in cases of fading or equipment problems; this is especially true for RSM type BSM that involve onboard route execution.

MPLS is likely to be used in a "network of network" scenario where label definition will have to be accommodated across the SI-SAP interface. Since labelled path are defined by extensions to RSVP, if the BSM accommodates RSVP it can also support MPLS label definition. (see recommendations in clause 10). For BSMs, the LSP defines a path in the satellite network that points to an uplink bandwidth allocation, a potential downlink beam allocation and an output port at the destination to continue its way in the Internet. In that case reservation requests from RSVP-TE must be processed at the ingress terminal or gateway and path semantics interpreted in the context of the satellite network.

Finally QoS routing in a BSM is a more challenging problem over a constellation where the constraints can also include power, channel impairments and field of view. This however is beyond the scope of the present document. Annex E lists some literature on the topic.

7.5.6 Multicast QoS management

Multicast is the topic of a specific Technical Report, TR 102 156 [14]. In this clause the general aspects of Multicast QoS are highlighted. Multicast in itself is covered under the general RSVP but is rarely used. Diffserv markings are also in principle compatible with multicast if receivers have negotiated how to handle them. But other models are necessary for multicast to be deployed within the BSM.

7.5.6.1 General model

QoS aspects that can be part of a multicast QoS management scheme include:

- general reliable multicast as a special form of QoS class. Guaranteed delivery can be considered as specific service parameter supported by the BSM. In this case all receivers get the same "guarantee" and receivers that have not subscribed to reliable delivery receive a lower QoS;
- QoS settings can be used for a multicast group or source. All members of the group then receive the same QoS for a given source or source ID. The source QoS setting adds another dimension to the multicast group management at the expense of some reservation complexity; and
- different receiver/destination hosts that can have different QoS settings. The same source may be available in different levels of QoS (bit rate, delay, jitter, etc.) and receivers "tune" to the QoS level they need. This involves complexity in the reservation process.

Details are available in [14].

7.5.6.2 MPLS/RSVP approach

In addition recent work in the field of Multicast QoS has defined that combining MPLS (and RSVP-TE) and RSVP to Diffserv markings can lead to efficient deployment of QoS in satellite multicast. This is the solution adopted in the IP ConferEncing with Broadband multimedia over Geostationary Satellites (ICEBERGS) project of the European Union IST Program.

7.6 Interlayer QoS functionality

It has been recognized by a number of IETF groups that when IP packets are transported over any wireless sub-network, the access device can have much better information about the behaviour subnetwork than any of the source and destination hosts especially about outages and degradations. This is especially true for BSM where all BSM edge elements (ST, gateway, satellite) as especially instrumented to survive link degradations. The idea of using layer 2 (or below) information violates the IP protocols assumptions that the two communicating endpoints should be in charge of the communication and adapt the transport protocols to events on the path, so interlayer communications has not been popular. However, the rapid development if IP-enabled wireless devices of all kind (from cellular to 802.11 to satellite) is making the use of link information more and more popular.

There is a need for signalling changes in BSM characteristics without waiting for end-to-end blind retransmissions based on peer transport retry timers. The issue then becomes how to modify or use current protocols to transmit that information back into source before for end-to-end mechanisms are triggered. While it is possible to do this using a protocol that is not IP the goal of the current work is to do it using IP protocol because of their wide deployment and technology independence. The proposed IETF Working Group TRIGTRAN recommends that the ensuing messages not be acknowledged (not a reliable protocol) so that the new protocols are more "advisory" than "mandatory" and the advised hosts may just discard the messages if they do not need it.

It is already embedded in routing protocols to signal "link up"/"link down" events what is needed now is to add to these control messages some bandwidth change, path changes etc.. There is also a need to know where are the other hosts that can receive that information, necessitating an interlayer host discovery mechanism. In addition the protocols themselves that are used to transmit the information have not been identified, although some candidates include:

- an ICMP message which was proposed in published work on the Lightweight Interlayer Signalling Protocol (LISP); see annex C;
- a unicast message to applications that request triggers;
- a multicast message to listening applications;

- inputs to the "path" computation in OSPF to avoid routing to a link with problems; and
- the use of RSVP "RESV Confirm".

As a response to such a message a host can do a number of actions:

- reducing TCP's congestion window;
- referring packets until additional event notifications arrive;
- notifying applications that an event has occurred;
- change traffic shaping parameters; and
- trigger the use of variable encoding and QoS renegotiations.

Some issues of how often the messages should be sent and the ripple effect over the rest of the network remain open.

7.7 QoS requirements summary

Table 11 presents a summary of BSM services, a preliminary QoS class (to be refined in one proposed TS) and the compliance of a BSM as an appropriate means of delivering the service at the QoS level specified.

Table 11: QoS-based services and BSM delivery

Service/protocol	QoS class	QoS Function	BSM delivery
RTP/UDP (VoIP, interactive application)	High	Low delay Lowest Jitter Low loss	Depends on BSM architecture
RTP/UDP with RTSP(Streaming Audio/Video)	Medium	Low delay Jitter can be compensated Low loss	Yes
RSVP (QoS Signalling)	Medium-High	Low delay Medium jitter Low loss	Required
HTTP/FTP/TCP (web traffic)	Medium	Medium everything	Required
SMTP (email)	Best effort	Best effort	Required

8 BSM IP availability and performance

8.1 Performance management

According to the ETR 309 [68], "Network Performance (NP) is the ability of a network or network portion to provide the functions related to communications between users; it contributes to service accessibility, service retainability and service integrity. Network performance parameter values are usually derived from Quality of Service (QoS) parameter values". In this clause we review the standardization of IP performance monitoring.

While QoS parameters are set using service, user and operator requirements, they must be measured in the network to ensure that they are met. There are financial consequences to meet or not to meet performance specifications. Since QoS and its management are is essential to next generation BSMs, systems that will not deploy it will not be able to be successful in the market. The management of QoS technologies provides the elemental building blocks that will be used for future business applications in service provider networks and enable:

- service improvement and gain;
- more users per terminal;
- new services offering; and
- financial gains from adequately negotiating and meeting Service Level Agreements.

In essence, capacity planning is probably the main reason why performance is measured at the IP level. Internet Service Providers usually buy trunk bandwidth as a lot of them do not own the infrastructure. In addition they need to plan capacity to establish capital investment in terms of routers and switches. The measured performance not only will provide the needed bandwidth and delay parameters but these parameters will assist network operations by supplying real time information for the NCC and supply engineering with data that cannot be found from the non real time network management systems. With the need for QoS to offer value-added service, performance and monitoring entities send reports to customers proving how QoS goals are met. Finally, with usage-based billing some measures are de facto needed to enable billing of individual customers.

8.1.1 Service Level Agreements (SLAs)

A network without predictable performance cannot be profitable. A major feature of the current Internet is the Service Level Agreement or SLA which is closely linked to Diffserv QoS management. It is a set of traffic management rules written as a contract between a subscriber and a service provider. It guarantees that the service provider will manage the traffic of that customer to guarantee a certain quality and performance (delay, bandwidth, availability etc). SLAs were originally designed for Frame Relay or ATM networks. The guarantees were then in terms of network availability and data-delivery reliability. In recent years, SLAs have moved to the Internet Service Providers and are now interacting directly with, for example, bandwidth brokers in Differentiated Services (Diffserv). SLAs are used to select traffic policy in token bucket traffic shaping and queuing parameters such as discard rules.

In the satellite world right now SLAs are very simple. Satellite network operators (wholesaler) supply a constant bandwidth (fat pipe) to each service provider. These in turn supply their STs some traffic contract usually in terms of guaranteed rate and best effort (with a peak rate). In the future QoS guarantees and more differentiated traffic classes could give rise to more sophisticated SLAs.

8.1.2 IP performance

As Internet traffic continues to grow exponentially, it has become essential for both the users and service providers to have a clear understanding on the performance of the network. The "Internet Performance Measurement and Analysis" (IPMA at the University of Michigan and Merit Networks) project studies the performance of networks and networking protocols in local and wide-area networks and allows users to download BGP table for monitoring. In addition "The National Laboratory for Applied Network Research" (NLANR) has as its primary goal to provide technical, engineering, and traffic analysis support of high speed networks and developed and supported the development of a number of performance tools. Finally the North American Network Operator Group (NANOG) maintains a mailing list and hosts frequent meetings to discuss IP level availability and performance.

The IETF via for example the Benchmarking Methodology (bmwg) [35] and the Internet Protocol Performance Metrics (IPPM) [42] has investigated IP performance for about 6 years. The ITU-T WGs 12 and 13 have current efforts for the measurement of IP QoS. ITU-T Recommendation Y.1541 [27] specifies IP performance values to be achieved internationally for each of the performance parameters defined in ITU-T Recommendation Y.1540 [26]. As seen in clause 8, ITU-T Recommendation Y.1541 [27] defines six different network Quality of Service (QoS) classes that are agreed between the end-users and the network providers.

Performance standards specify procedures for measuring an individual metric and specify why this metric is important to verify the behaviour of the network as regard to a QoS feature. Metrics must be "carrier class": information can be gathered by network operators or testing groups not just end users. It is important for operators to work closely with their customers on designing useful measurements. These measurements will be applied to the quality, performance, and reliability of Internet data delivery services, hence are clearly related to QoS. They must provide unbiased quantitative measures that in turn can be used in billing systems and to verify Service Level Agreements (SLAs), see clause 8.1.1). What operators need are industry-wide, unambiguous and quantitative reporting of network behaviour. Since performance is also part of the whole network management operations, it is also important for measured performances to be included in Network Management Information Bases (MIBs) for easy access by standard management systems.

8.1.3 BSM performance

The BSM performance management needs to put emphasis on manageable and measurable parameters hence a quantitative vs. qualitative approach and evaluate how and where the QoS parameters metric should be measured. In turn effective performance monitoring should help in establishing and enforcing policy management.

In BSMs, performance and availability are usually directly liked to the characteristics of the satellite transmission (physical and link layer) that directly affect the BSM capabilities to operate. BSM propagation times may prevent low end-to-end delay requirements from being met. However, ITU-T Recommendation Y.1541 [27] states: "Every network provider will encounter these circumstances and the range of IPTD objectives provides achievable QoS classes as alternatives". This opens areas of future work for the BSM.

The challenge for the accurate BSM availability and performance measurements is to relate lower layer parameters to end-to-end network parameters. Hence BSM performance needs to be measured at different levels to support the network management structure:

- application level - where the QoS parameters are specified and where the some of the packet level performance will be measured; for the BSM this means at the entry and exit of the SI layer at source and destination;
- network level/ISP - where the QoS is guaranteed end-to-end and where flow-level monitoring can happen - for the BSM this may mean from ingress SI to egress SI but also from source to destination. This also includes some Performance Enhancing Proxies (PEPs) at layer 4 (see clause 8.3.3); and
- satellite operator level/lower layers - this is where the fundamental link and MAC layer monitoring is done and mostly SD.

The issue for BSM is how to communicate satellite link faults to other peering networks on solution would use Border Gateway Protocol Extensions or ICMP extensions but it needs to be investigated further. The performance API between the BSM world and the IP world can clearly be located at the Satellite Independent/Service Access Point (SI-SAP).

8.2 Performance management functions

The major BSM performance management functions do not differ in essence from those of the terrestrial networks. They are usually at or above the IP layer. As BSM evolve, there will be more performance management in the ST, the satellite and the gateways. For example the application of Diffserv classes allow to improve the performance of near real-time traffic. Closer coupling between RSVP (and Intserv in general) with BoD algorithms can reduce delay and the risk of queue overflow (both in the ST and onboard). The possibility to modify traffic shaping and admission parameters with BSM behaviour as well as with the demands of higher level signalling will also reduce loss and even trigger reroutes when conditions go bad. This clause only highly the salient features of Performance Management Functions.

8.2.1 Admission Control

Admission control is for connection oriented traffic classes or traffic classes that have predictable behaviour. Connection Admission Control (CAC) or Call Admission Control is the set of actions taken by the network at a connection set up phase or during the connection re-negotiation phase in order to establish whether the connection can be accepted or should be rejected. CAC were originally designed for ATM but their concept can be extended to any session-based protocol that requires guarantees of QoS (availability, bit rate, delay etc.). In essence, it is a function that determines whether the local network node has sufficient available resources to supply the requested QoS of a session. The Admission Control (AC) algorithm ensures that the network takes the actions necessary to enforce network admission policies and as such influences values of leaky bucket parameters and of congestion control mechanisms. It is usually based on the estimation of effective bandwidth and other traffic management concepts.

8.2.1.1 Admission Control parameters

Admission control parameters vary but will include the typical traffic descriptors (bandwidth, acceptable delay and loss, level of jitter tolerance). It may also include the source and destination of the admitted traffic, a duration for which the admission is valid, the location of the sender and receiver etc. All these parameters are used to determine if the new flow (or call) can be served by current network resources and offered load. However, no quantitative loss or delay guarantee to aggregate traffic can be efficiently accomplished with existing static bandwidth allocation methods, which assume some stochastic model on the input traffic arrivals. This is an active area for research.

8.2.1.2 Adaptive Bandwidth Control

In an aggregate traffic management and control framework, efficiently allocating bandwidth to provide quantitative QoS has been difficult due to unpredictable, unknown statistical characteristics of aggregate traffic. With inaccurate traffic information, static bandwidth allocation results in the network being underutilized. An alternative is to use Adaptive Bandwidth Control (ABC), whereby the allocated bandwidth is adjusted over time to maintain QoS metrics of interest, including the average queue length, packet loss, or packet delay.

8.2.1.3 Admitting a session in the BSM

For the BSM, admission control crosses the SAP: it has some SIAF and SDAF module. The SI part of the admission control module may also have to communicate with the NCC for global admission policies and the SD part with the satellite (if RSM) to ensure that there is no congestion onboard.

Traditional admission control in the satellite networks is fairly static. The ST is admitted at logon and is based static bandwidth measurements. Parameters can only be changed by under administrative control usually not with the dynamics of the traffic and the satellite network behaviour.

Recent work however makes it possible for the BSM, in addition to "traditional" parameters to include the following parameters in Admission Control:

- availability;
- channel level information and satellite energy conservation policies; and
- long range weather estimation; this is particularly interesting to evaluate actual capacity and fading for Ka band BSM.

Admission control can result in some policy settings being sent back to the ST or (as shown in figure 16) generate a scheduled reservation that will be used for the admitted traffic. The CAC can be integrated to the BSM authentication/logon procedures and should allow some changes as conditions change. However AC is not used for dynamic settings (packet level) but for longer range predicted traffic (least flow level or label level in MPLS).

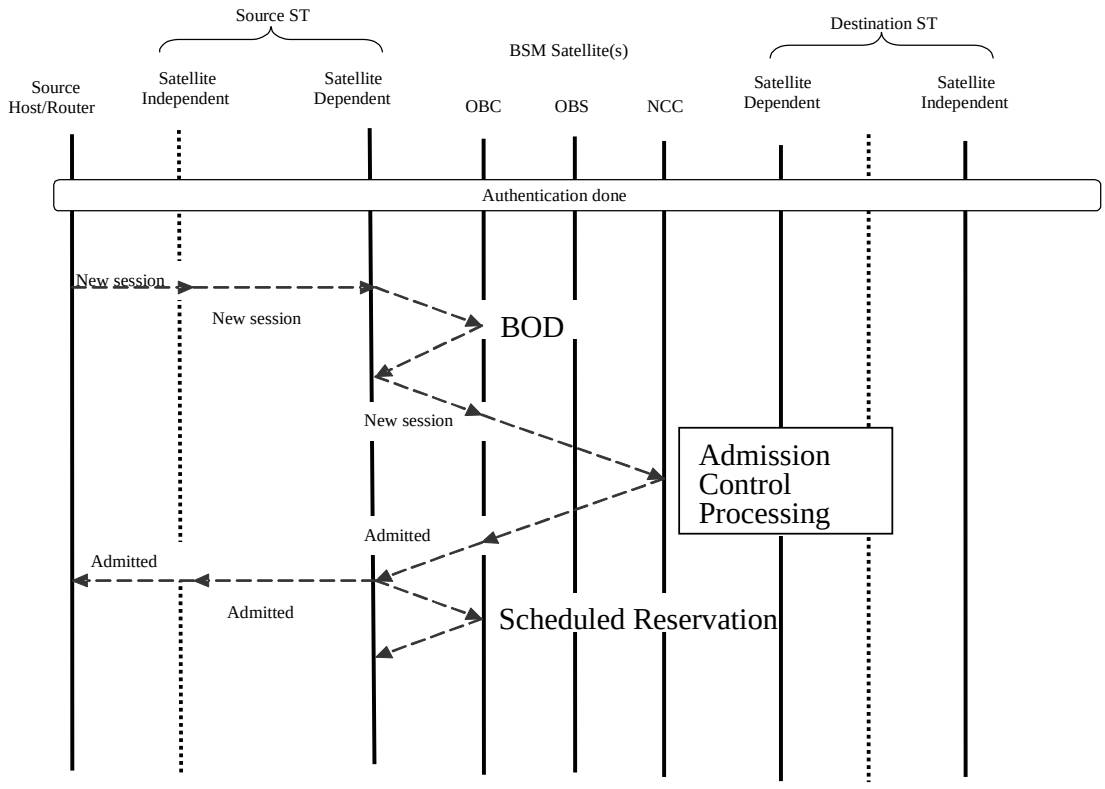


Figure 16: Admission Control process for RSM

8.2.2 Flow control

Flow control is usually for non admitted classes, those classes that have non predictable behaviour, in essence connectionless best effort traffic classes. Hence it is designed for networks where individual connections do not reserve bandwidth and for the best-effort traffic. It usually uses a round-robin-like queue service discipline in the traffic queues and window-based transmission mechanisms. The Transmission Control Protocol (TCP) flow control and congestion avoidance is described in clause 8.3.

8.2.3 Traffic shaping

Before entering the network, traffic is queued. Traffic between queues is managed by queuing mechanisms (see next clause). Traffic Shaping imposes a limit to the admitted load in the network within a queue. Traffic Shaping in effect performs a local admission control function. Figure 17 shows how shaping polices traffic and limits subscribers to their committed rates in the network.

In the access network when flat rate billing is used, networks are usually oversubscribed to ensure that resources are always occupied. In that case the policing and shaping of traffic ensures that no customer consumes more resources than what they have signed to pay for in the SLA. The shaping parameters are usually fairly static but all models allocate for some dynamic variations.

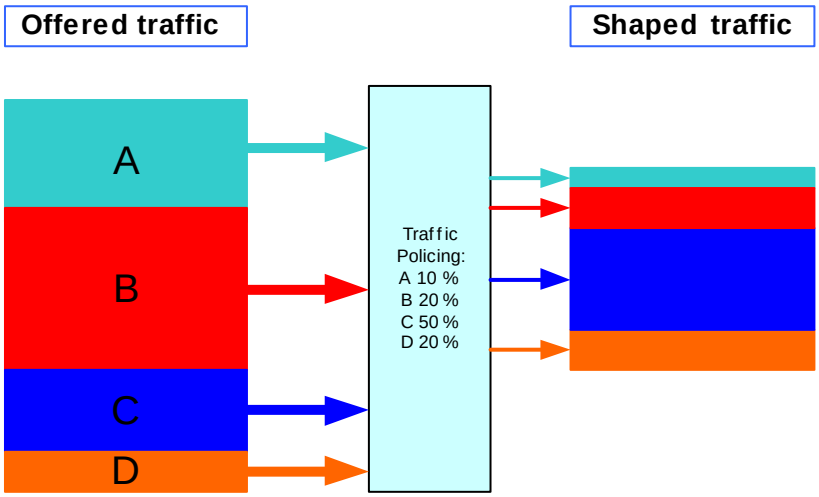


Figure 17: Traffic shaping

In the BSM the DAMA algorithms inherently shape the traffic on uplink but in the ST (or gateways) other shaping and policy mechanisms can be used based on IP and/or ATM traffic management.

8.2.3.1 Token Bucket/Leaky Bucket

Traffic shaping algorithms include the "Leaky Bucket" and the "Token Bucket" algorithms. In the leaking bucket algorithm the drip rate of the "bucket" defines the rate at which the queue can empty. In the token bucket it is the generation of tokens that limit the rate of transmission. A packet will leave the queue only if there is a "drop" or "token" available. If there is none then the packet is marked "out-of profile". In times of low loads when there is no congestion in the network, the out-of-profile packets are transmitted and increase the instantaneous throughput of the network. In times of congestion the out-of-profile packet are discarded.

8.2.3.2 Policy control

Policy control is a function that determines whether a user has administrative permission to reserve network resources at a node. In the BSM it is an NCC function and relates to security and authentication. It will not be addressed here.

8.2.3.3 Link between traffic shaping and BOD

In a BSM it is important that the traffic shaping parameters on the SI side of the ST be matched to the transfer capacity defined by the actual allocated bandwidth. Then the ST queue can empty at the right rate to fill all allocated slots and allow the congestion algorithms to be triggered in times where the allocated bandwidth is low.

8.2.4 Queuing and congestion avoidance

In a router or switch, shared resources need to be distributed amongst competing customers according to contention resolution policies. This is the role of the queuing policies. To a rough approximation queue management algorithms manage the length of packet queues by dropping packets when necessary or appropriate, while scheduling algorithms determine which packet to send next and are used primarily to manage the allocation of bandwidth among flows.

8.2.4.1 Explicit Congestion Notification (ECN)

Explicit Congestion Notification has heritage from the ATM Cell Loss Priority (CLP) bit. It was shown in clause 7.5.2.1 as two bits following the 6 bits of the DSCP. The use of the 4 ECN levels was defined in RFC 3168 [62]. Many protocols (including TCP) use packet drop as an indication of congestion. With the addition of active queue management (clause 8.2.4.2) to the Internet infrastructure, routers can detect congestion before the queue overflows. Hence, routers are no longer limited to packet drops as an indication of congestion and can instead set (or "erase") the ECN bits in the packet headers when congestion is detected. At destination, the marked packets can then either be dropped or forwarded to their destination depending on the local policies.

8.2.4.2 Active Queue Management (AQM)

Queues are used to smooth spikes in incoming packet rates and to allow the router sufficient time for packet transmission. When the incoming packet rate is higher than the router's outgoing packet rate, the queue size will increase, eventually exceeding available buffer space. When the buffer is full, some packets will have to be discarded.

Active Queue Management (AQM) refers to the set of mechanisms that is used to prevent packet loss due to buffer overflow. A straightforward solution is to drop the packets that are just arriving at the input port; that is, if a packet arrives and finds the queue full it will be dropped: this is the tail drop policy. Other solutions include dropping the first packet in the queue, dropping a random packet already stored in the queue (RED, see below).

8.2.4.2.1 Early Packet Discard (EPD)

Early packet discard comes from ATM and is implemented in the output ports of a router or switch. Early packet discard keeps track of the passage of frames (ATM cells) on selected flows or virtual circuits. If a new frame begins when the occupancy of the link buffer is above a threshold value, it discards the frame hence the packet.

8.2.4.2.2 RED and WRED

Random Early Discard (RED) is a buffer management scheme designed to prevent tail drop caused by large traffic bursts. RED will randomly selects and drop packets in a queue. This prevents tail drop that can lead to traffic oscillation in the network. RED however has to be used on aggregated flows [19]. Weighted RED (WRED) uses packet markings when dropping packets.

8.2.4.3 BSM impacts

Congestion control can and will be applied at every queue in the BSM (SI, SAP, OBP, gateway). If congestion control is implemented at the ingress/egress to the BSM (ST or gateway) standardized functions can be used. In an OBP simple methods are to be used. The simplest method will be queue drop, which means that all packets are discarded when a queue goes above a preset threshold.

In BSMs because of the level of aggregation at the ST, ECN is more likely to be more effective than RED. Recent work on RED over satellite has confirmed that in certain cases RED performs poorly in ST queues because in fact each queue represents a single flow.

In addition for RSM type BSM, the choice of onboard queuing policy will be influenced by the level of aggregation. If onboard queuing is by destination but QoS class aggregation is still large enough, RED could be used at the expense of higher complexity (virtual QoS class queuing). If not, explicit congestion notification (ECN) will be applied on individual packets in a queue.

The adaptation function in an ST should be able to map an ECN bit into a SDU so that in case of congestion anywhere in the BSM, including onboard, packets can be dropped according to a preset policy.

8.2.5 Scheduling

Queuing and scheduling mechanisms allow controlling congestion by determining the order in which packets are sent out from a queue to an interface based on priorities assigned to those queues and packets. Scheduling policies are defined by QoS requirements amongst each customer flow and determine the scheduling of each packet, its relative priority when awaiting service. There are a large number of scheduling protocols, each of which enable the creation of different types of queues, affording greater or lesser degrees of differentiation of traffic, and to specify the order in which that traffic is sent.

8.2.5.1 Round Robin and weighted round Robin

Round Robin is the simplest scheduling algorithm. Resources are allocated to each requesting queue, in turn. After resources are depleted, the next round of allocation starts where the previous one stopped, thus ensuring that all queues will eventually get service. Weighted round Robin is a variant where some queues will be serviced more often (or with more resources) than others based on a "weight" representing some form of priority. Weighted round Robin leads to different scheduling classes.

8.2.5.2 Weighted fair queuing

The principle between weighed fair queuing is simple. Resources are allocated between requesting queues by first allowing interactive applications at the head of the queue to reduce delay and then allocating the remaining resources to the other queues.

8.2.5.3 BSM scheduling

Scheduling in the BSM is intrinsically linked to the way the system manages bandwidth and other scare resources. At the macro level at the NCC, each ST can be considered a "requesting queue" and transmission opportunities (and bandwidth allocation) will be assigned by a well known algorithm based on the type of ST, while ensuring fairness amongst peer STs. At the ST level, transmission scheduling will be managed across queues based on local traffic parameters. Scheduling, like other traffic related function is thus intrinsically linked to how the SAP requests and allocates satellite bandwidth. Table 12 summarizes the performance management functions available to the BSM.

Table 12: Summary of admission/flow/congestion control

Function	Protocol
Packet marking	ECN
Admission	CAC RSVP
Policy and shaping	Leaky bucket Token bucket
Queuing and scheduling	Weighted fair queuing Weighted round Robin Class based queuing
Congestion avoidance	TCP algorithms RED and variants

8.3 TCP performance

The Transport Control Protocol (TCP) is a reliable (acknowledged) protocol widely used over the Internet and its use over different networks including satellites is well known. Because its operation has a great impact on the service that relies on it, TCP operations are described in this clause. While a number of variants of TCP have been standardized this clause uses the characteristics of TCP-Reno (the original was TCP-Tahoe and improvements on bandwidth usage have been named New -Reno and Vegas).

8.3.1 TCP congestion control

TCP employs four congestion control mechanisms slow start, congestion avoidance, fast retransmit and fast recovery. These algorithms are used to adjust the amount of unacknowledged data that can be injected into the network and to retransmit segments dropped by the network. They are closely linked to the window based flow control of TCP. TCP uses two variables for congestion control:

- the congestion window (cwnd) is the upper bound on the amount of data the sender can inject into the network before the reception of an ACKnowledgment (ACK). The value of cwnd is limited to the receiver's advertised window and can be increased or decreased during a session depending on the amount of perceived congestion in the network; and

- the slow start threshold (ssthresh) determines which algorithm is used to increase the value of cwnd. If cwnd is less than ssthresh the slow start algorithm is used to increase the value of cwnd. However, if cwnd is greater than or equal to (or just greater than in some TCP implementations) ssthresh the congestion avoidance algorithm is used. The initial value of ssthresh is the receiver's advertised window size. Furthermore, the value of ssthresh is set when congestion is detected.

8.3.1.1 Slow start and congestion avoidance

TCP is based on the principle that a sender ignores the status of the network. In order to avoid transmitting too much traffic and create un-necessary congestion, TCP uses the "slow start" algorithm. In slow start the cwnd is set to 1 segment (in essence 1 packet) and ssthresh is set to the receiver's advertised window. Each time a packet is ACKed cwnd is increased by 1 segment. Slow start goes on until cwnd reaches ssthresh or there is loss. At or above ssthresh "congestion avoidance" is used. Under that condition, cwnd can only increase by 1/cwnd for each incoming ACK resulting in a much lower growth. If there is loss then sstresh is set to half of cwnd and cwnd is reset to 1. And slow start restarts.

8.3.1.2 Fast retransmit and fast recovery

TCP ACKs always acknowledge the highest in-order packet that has arrived. So an ACK for packet N also ACKs all segments sent before N. Also if a segment is received out-of-order the ACK will be for the highest in-order segment not the segment was received. The "fast retransmit" algorithm uses duplicate ACKs to detect lost segments and retransmits the missing segment without waiting for a time-out, thus avoiding to go back to slow start mode. After fast retransmit, the fast recovery algorithm is used to adjust the congestion window. First, the value of ssthresh is set to half of the value of the current cwnd and cwnd is also halved. The value of cwnd is then increased by one segment for each duplicate ACK that has arrived, hence one segment that has left the network; this is an artificial inflation based on packet that have left the network. When the cwnd permits, TCP is able to transmit new data. This allows TCP to keep data flowing through the network at half the rate it was when loss was detected. When an ACK for the retransmitted packet arrives, the value of cwnd is reduced back to ssthresh, which is half the value of cwnd when the congestion was detected.

8.3.1.3 Selective acknowledgements

Selective Acknowledgements addresses the transmission limitations of TCP. A Selective ACKnowledgment (SACK) mechanism was defined in RFC 2018 [37]. With TCP SACK, the data receiver can inform the sender about all the segments that have arrived successfully, allowing the sender to retransmit only the segments that have actually been lost.

8.3.1.4 Window scaling

In large delay × bandwidth product networks, the initial fixed windows of early versions of TCP, were preventing the channel to fill to capacity as:

$$TCPwindow = delay \times bandwidth$$

RFC 1323 proposes to use window scaling to ensure that the full available bandwidth is used. This is now a feature of all TCP implementations.

8.3.2 TCP operations over BSM

TCP was on of the first Internet protocols that was analysed for transmission over satellites. TCP usage over satellite is standardized in RFC 2488 [46]. The next clauses describe the impacts of satellite transmission over satellite.

8.3.2.1 Consequences of noise

If TCP ignores why a packet was dropped: congestion or corruption? TCP must assume the drop was due to network congestion; this is by design and to avoid congestion collapse upstream in the network. TCP's default mechanism to detect dropped segments is a timeout (Retransmission Time Out or RTO). If the sender does not receive an ACK for a given packet within the RTO the segment will be retransmitted, TCP will then use the lost segment as an indication of congestion in the network and trigger the use of the slow start algorithm. Therefore, packets dropped due to corruption cause TCP to reduce the size of its window and decrease throughput significantly, even though these packet drops do not signal congestion in the network. The use of fast retransmit and fast recovery will help alleviate these problems.

8.3.2.2 Consequences of delay

In addition to the widow issue highlighted above, large delays have also other impacts on the behaviour of TCP. The slow start and congestion control algorithms can force poor utilization of the available channel bandwidth when using long-delay networks. For example, transmission begins with the transmission of one segment. After the first segment is transmitted the data sender is forced to wait for the corresponding ACK. When using a GSO satellite this leads to an idle time of roughly 500 ms when no resources are used. Therefore, slow start takes more time over BSMs than on typical terrestrial channels. This holds for congestion avoidance, as well. The "Endpoint Congestion Management" working group at the IETF has studied these issues and proposed solutions applicable to many transport mechanisms based on received traffic. In addition, Performance Enhancing Proxies (see next clause) can alleviate this problem.

8.3.2.3 Recommended mechanisms

Table 13 from RFC 2488 [46] presents the recommendations for using TCP over satellite.

Table 13: Mechanisms for TCP over satellite defined in RFC 2488 [46]

Mechanisms	Location	Use
Slow Start	Sender	Required by the protocol
Congestion Avoidance	Sender	Required by the protocol
Fast Retransmit	Sender	Recommended
Fast Recovery	Sender	Recommended
Window Scaling	Sender and Receiver	Recommended
Protection Against Wrapped Sequence space	Sender and Receiver	Recommended
Round Trip Time Measurements	Sender and Receiver	Recommended

8.3.3 Performance Enhancing Proxies

Performance Enhancing Proxies (PEPs) are defined in RFC 3135 [60] and are used to improve the performance of TCP (TCP-PEPs) or other protocols over network paths where typical performance suffers due to characteristics of a link on the path. Different types of PEPs are available depending where they operate in the network stack:

- transport layer PEPs operate at the transport level; they do not modify the application protocol in any way, but let the application protocol operate end-to-end. TCP-PEPs are transport level PEPs; and

- application layer PEPs operate above the transport layer they include proxies and caches they try to improve performance or service availability and reliability.

In this clause a number of transport PEPs are reviewed, for TCP and UDP. It also mentions the use of caching to improve end-to-end delay. Proxies are discussed in the recommended BSM protocol manager.

8.3.3.1 Split connections and TCP spoofing

The term TCP spoofing is sometimes used synonymously for TCP PEP. The term TCP spoofing more accurately describes the characteristic of intercepting a TCP connection in the at the entry point to the link under consideration and terminating the connection as if this point was the intended destination. This creates in effect a split connection TCP implementation. It terminates the TCP connection received from an end system and establishes a corresponding TCP connection to the other end system. This is sometimes referred as ACK spoofing because the source will get an ACK on a packet that is not yet at its intended destination. It also enables other ACK manipulations such as ACK spacing to control the flow of packet across the network. The after the split connection the path may be continued by using a TCP connection optimized for the link or another protocol. TCP spoofing will be used in order to address a mismatch in TCP capabilities between two end systems. On large delay bandwidth this will increase the efficiency of TCP. However it is incompatible with security protocols like IPSec which hide the information necessary for the interception except if the ST where the interception is done is considered a trusted entity.

8.3.3.2 TCP bandwidth snooping

Bandwidth snooping is another transport level performance enhancing proxy. It is a valid mechanism on all networks that use one form or another of bandwidth on demand. BoD requires time between assignments and in reality limits cwnd to the current allocated bandwidth even if the queue is still growing and more packets need transmission. As a consequence TCP will move between cycles of slow start and congestion avoidance until it reaches full bandwidth, with the associated delays (figure 18). In some cases active bandwidth management is required to alleviate this effect and minimize delay during slow start ramp-up. It is based on inferring the needed capacity (by knowledge of the application, by monitoring the queue etc.) and in times of growth slight over-requesting capacity. The amount of the request can be found by using predictive methods or by slightly over allocating bandwidth. This results in a better utilization of the resources and higher end-to-end TCP delay performance. The disadvantages are higher BoD algorithm complexity and the risk of over-allocation.

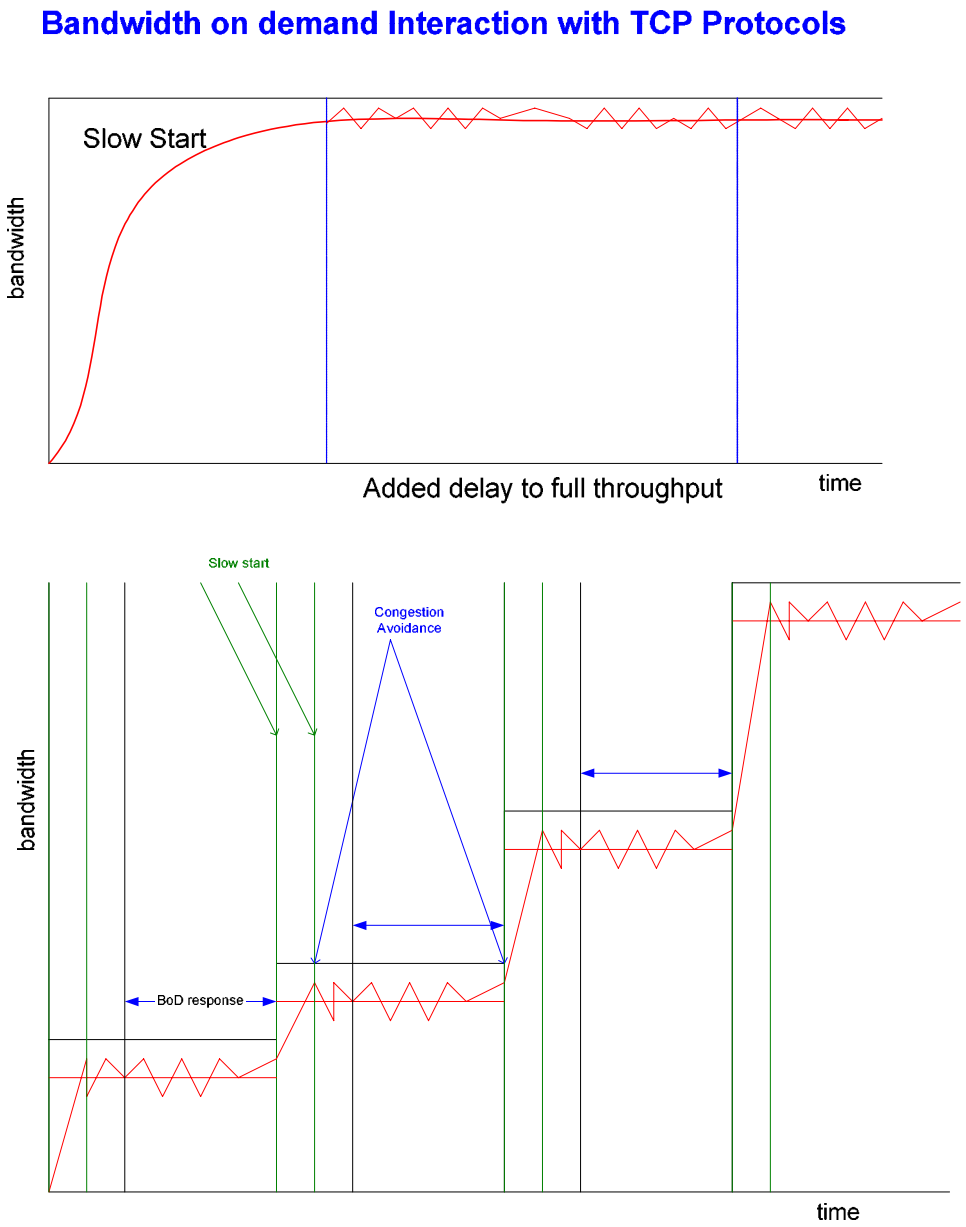


Figure 18: TCP Bandwidth snooping

8.3.3.3 TCP Friendly Rate Control (TFRC)

The TCP Friendly Rate Control protocol, defined in RFC 3448 [65] was designed for streaming and audio streams competing with TCP traffic. TFRC is a congestion control mechanism that could be used with RTP. It is one example of a transport level PEP that is not TCP. TFRC allows those flows that compete with TCP to be somewhat limited in their bandwidth consumption, an important feature when thinking of future usage of the Internet for more video and live broadcast. TFRC does not change RTP but uses receiver statistics and throughput equations to limit the transmission rate of the source. It is well suited for large server, smaller client transfer models and can be extended to the multicast environment. Implementation details are available in [65].

8.3.3.4 Caching

Caching is an application level PEP. It defines the storage of information that is updated infrequently close to the point of usage of that information. Hierarchical organization of caches is commonly used in the World Wide Web for anything from catalogues and company information. Web caching has been recognized as an important vehicle to mitigate web traffic explosion. The main objective being to overcome the delays created by communications among servers and attempting to improve the response times experienced by end-users. In satellite networks caching has proven to greatly improve end-to-end delay and reduce the number of web accesses across the network backbones and the congestion in some widely accessed sites. Even with Internet applications becoming increasingly diverse in their QoS requirements caching policies are still very important and more and more include QoS requirements. Present caching approaches optimize aggregate metrics such as URL hit rate or byte hit rate, it is also possible to have per-client-class or per-traffic-class QoS requirements that are individually met.

8.4 Standardized performance metrics

In order to set the performance monitoring specifications performance metrics need to be defined and assigned some agreed on value either based on the actual service requirements or IP specific parameters (based on aggregated service requirements).

8.4.1 Service performance requirements

The ITU has defined and standardized service requirements which are the basis for all network performance [25]. They are presented in table 14 for audio and video transmission and table 15 for data applications. As can be seen from these tables the BSM performance were not taken into account. While it is true that low delays may lead to better overall "quality" some delay goals may not mean a BSM is de-facto non-compliant. For example the 200 ms delay for telnet would mean that no BSM could support that service. However there has been use of telnet over satellite and while it is slow it is not impossible to use. The performance goals of tables 14 and 15 must be taken as "illustrative" in the BSM context and give support for a BSM specific set of performance parameters as will be recommended in the conclusion to the present document.

Table 14: Performance targets for audio and video applications from ITU-T Recommendation Y.1540 [26]

Medium	Application	Degree of symmetry	Typical data rates	Key performance parameters and target values			
				One-way delay	Delay variation	Loss	Other
Audio	Conversational voice	Two-way	4 kb/s to 64 kb/s	< 150 ms preferred < 400 ms limit	< 1 ms	< 3 % Packet Loss Ratio (PLR)	
Audio	Voice messaging	Primarily one-way	4 kb/s to 32 kb/s	< 1 s for playback < 2 s for record	< 1 ms	< 3 % PLR	
Audio	High quality streaming audio	Primarily one-way	16 kb/s to 128 kb/s	< 10 s	< 1 ms	< 1 % PLR	
Video	Videophone	Two-way	16 kb/s to 384 kb/s	< 150 ms preferred < 400 ms limit		< 1 % PLR	Lip-synch: < 80 ms
Video	One-way	One-way	16 kb/s to 384 kb/s	< 10 s		< 1 % PLR	

Table 15: Performance targets for data applications from ITU-T Recommendation Y.1540 [26]

Application	Degree of symmetry	Typical amount of data	Key performance parameters and target values		
			One-way delay	Delay variation	Loss
Web-browsing - HTML	Primarily one-way	~10 kB	Preferred < 2 sec/page Acceptable < 4 sec/page	N.A	TBD
Bulk data transfer/retrieval	Primarily one-way	10 kB to 10 MB	Preferred < 15 sec Acceptable < 60 sec	N.A	TBD
Transaction services	Two-way	< 10 kB	Preferred < 2 sec Acceptable < 4 sec	N.A	TBD
Command/ control	Two-way	~ 1 kB	< 250 ms	N.A	TBD
Still image	One-way	< 100 kB	Preferred < 15 sec Acceptable < 60 sec	N.A	TBD
Interactive games	Two-way	< 1 kB	< 200 ms	N.A	TBD
Telnet	Two-way (asymmetric)	< 1 kB	< 200 ms	N.A	TBD
E-mail (server access)	Primarily one-way	< 10 kB	Preferred < 2 sec Acceptable < 4 sec	N.A	TBD
E-mail (server to server transfer)	Primarily one-way	< 10 kB	Can be several minutes	N.A	TBD
Fax ("real-time")	Primarily one-way	~ 10 kB	< 30 sec/page	N.A	$< 10^{-6}$ BER
Fax (store & forward)	Primarily one-way	~ 10kB	Can be several minutes	N.A	$< 10^{-6}$ BER
Low priority transactions	Primarily one-way	< 10 kB	< 30 sec	N.A	TBD
Usenet	Primarily one-way	> 1 MB	Can be several minutes	N.A	TBD

8.4.2 IP performance metrics

This clause briefly describes the basic performance measurements for Internet traffic, hence for aggregated services. These metrics were defined in the RFC 2330 [42], RFC 2678 [50] and ITU-T Recommendations Y.1540 [26] and Y.1541 [27] and are used to manage traffic in IP networks. They can be summarized in two categories: link metrics and per packet/flow measures.

8.4.2.1 Link metrics

Link metrics relate to end-to-end and system level capabilities. They include (but are not limited to):

- connectivity/reachability: connectivity verifies if there a connection between 2 hosts; the polling all devices in less than 60 sec (for 10 000 devices) is a design criterion used by NANOG;
- bulk transport capacity: this is measured in bps and is based on the aggregated physical characteristics of the host;
- link bandwidth capacity: in effect the bandwidth of the host interfaces;
- throughput: this measures the number of packets delivered to the egress output port; and
- network availability: this is measured in percentage or second/minutes of outages; the ITU-T Recommendation Y.1540 [26] recommends relating it to loss ratio.

8.4.2.2 Per packet and per flow measures

Table 16 lists performance objectives for IP QoS classes based on ITU-T established Diffserv classes presented in table 4.

Table 16: QoS class definitions and network performance objectives from ITU-T Recommendation Y.1231 [28]

		QoS Classes					
Network Performance Parameter	**Nature of Network Performance Objective**	**Class 0**	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5 Un-specified or Unbounded**
IP packet transfer delay IPTD	Upper bound on the mean IPTD	100 ms	400 ms	100 ms	400 ms	1 sec	U
IP packet delay variation IPDV	Upper bound on the 1 - 10^{-3} quantile of IPTD minus the minimum IPTD	50 ms	50 ms	U	U	U	U
IP packet loss ratio IPLR	Upper bound on the packet loss probability	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	U
IP packet error IPER	Upper bound	10^{-4}					U
NOTE: An evaluation interval of 1 minute is provisionally suggested for IPTD, IPDV, and IPLR, with 1 500 bytes packets and in all cases the interval must be reported.							

Per packet measures follow individual packets or flows ("population of interest" [26]) through the network and are in fact the best known:

- IP packet Transfer Delay (IPTD): this measures one-way and round trip packet transfer delay and is measured between a source and a destination; this can be defined over a single packet or flow of packets or a smaller group of individual packets (average delay);
- IP packet Delay Variation (IPDV): this is the average delay variation (jitter) and it measures the difference in arrival time between packets of the same group;
- IP packet ERror (IPER) or packet Error Ratio: the number of packets received with residual errors during a specified time interval or after the reception of a specified number of packets;
- IP packet Loss Ratio (IPLR): this is the loss metric, the number of packets lost during a specified time interval or after the reception of a specified number of packets; and
- goodput: the bit rate delivered to the application.

Other metrics include:

- spurious packets and out of order packets: measures the number of packet received out of order and may indicate congestion in the network; this relates to packet reordering as out of order packets can be re-ordered without loss but with added delay; and
- loss patterns: this is measured over a fairly long period of time and will indicate times or location of network problems.

Delay, jitter and loss are usually the most common metrics and are specified in SLAs and other QoS related functions.

These metrics are evaluated using a number of tools including dummy packets, traps, OS level commands (ping, rmon etc.).

8.4.3 BSM performance metrics

The BSM uses the same metrics as were defined in the previous clause but will apply specific BSM methods to their measure and monitoring. This clause defines the BSM metrics and how monitoring is performed. Annex D lists the IP performance metrics and their characteristics.

8.4.3.1 Link metrics

For the BSM the monitored link level metrics include connectivity, availability, loss and throughput.

8.4.3.1.1 Connectivity

The loss of connectivity in the BSM can mean three things: the link failed (or is in fading), the hardware failed or the software failed. In any case for a BSM fault detection has to do with the Satellite Control stations for the space segment and local connectivity managers for the ST. The former has a heritage of over 50 years and the latter has heritage in VSATs, satellite television terminals and cable set-top boxes. This is where interlayer methods may have the greatest impact on BSM performance management by allowing link level measures to be translated into manageable entities.

8.4.3.1.2 Availability

According to the ETR 309 [68], "Availability performance is the ability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided". Alternatively, availability can be loosely defined as the percentage of the time the satellite performs at the nominal capacity. Availability is measured as the probability that the network operates at nominal performance. It can also be measured in terms of the number of minutes the network does not operate at nominal levels.

Availability in turn drives the BSM satellite link budget. But the BSM availability is more than just air interface. ITU-R Recommendation S.1424 [23] has defined availability for Fixed Satellite Services (FSS) carrying ATM that can be taken as a guideline for the IP required availability. This availability follows a Hypothetical Reference Digital Path (HRDP) in the FSS (as ATM is connection oriented) and takes into account that the satellite (hence BSM) conforms to ATM performance goals of the I-356. The availability is defined as [23]:

$$A_{satellite\ HRDP} = A_{link} \times A_{earth\ station} \times A_{spacecraft}$$

where:

- A_{link}: availability component due to uplink and downlink rain attenuation and interference effects;
- $A_{earth\ station}$: availability (equipment reliability) of all transmit and receive earth station equipment up to the terrestrial interface;
- $A_{spacecraft}$: total availability (equipment reliability) of the spacecraft;
- $A_{satellite\ HRDP}$: product of all availability components on a satellite link.

It concludes that the yearly availability of a satellite HRDP (one direction) in the FSS should be greater than 99,85 % to be able to carry all ATM traffic. This translates in over 100 000 errored seconds per year or 30 hours per year. For the earth stations it proposes an availability figure of 99,95 % of the year (slightly above 10 000 seconds or 3 hours). This is lower than industry reliability for carrier-class systems (5 nines or 99,999 %).

The "variable" availability of the BSM can be used in performance management. Some traffic classes (and admission control) define availability in addition to delay and loss profiles. Hence the instantaneous availability figures can be used to manage which class of traffic can be sent over the BSM.

Finally in QoS routing there is the notion of alternate routing as was described in clause 7.5.5.1.1. Each of these routes (from 1 to n) may have a different availability due to the use of an alternate link or an alternate HRDP.

In that case:

$$ABSM = \max(A_{satellite\ HRDP1}, A_{satellite\ HRDP2} \ldots A_{satellite\ HRDPn})$$

Where max is the maximum function hence returns the maximum value of $A_{satellite\ HRDPi}$.

8.4.3.1.3 Throughput

Throughput defines the effective data transfer rate in bits per second for a particular service user as measured at the egress point of the network. Throughput is influenced by bandwidth sharing policies and overhead due to signalling and added overhead.

BSM throughput is usually measured as the number of cells/packets that cross the SI/SAP interface. There is often confusion in the terrestrial network about what a N Mbps BSM session means: does it or does not it include BSM specific segmentation and layering information? Hence a standard may be needed.

8.4.3.1.4 Goodput

Goodput defines the effective data rate delivered to the application. Goodput is influenced also by overhead and signalling but especially by reliable protocols that rely on acknowledgement. It can happen that while throughput is high goodput could be very low.

8.4.3.2 Packet/flow metrics

8.4.3.2.1 Delay

Delay is measured as the time in transit of a packet between the ingress of the network to the egress of the network. For the BSM it could be measured at the SI or the SI/SAP interface.

8.4.3.2.2 Delay variation (1 point and 2 points)

Delay variation (jitter) is a measure the differences in delay between the arrival of successive packet from the same flow at the egress of the network (1 point delay variation) or via a transit point (2 point delay variation). It can be controlled for those services that are sensitive to it by use of buffering and other more complex methods.

IP delay variation is defined as:

$$IPDV = IPTD_{upper} - IPTD_{\min},$$

where:

- $IPTD_{upper}$ is the $1\text{-}10^{-3}$ quantile of the IP Transfer Delay (IPTD) in the evaluation interval;
- $IPTD_{min}$ is the minimum IPTD in the evaluation interval (usually 1 minute with 1 500 bytes packets).

8.4.3.2.3 IP Loss Ratio

As for availability loss in the BSM can have multiple sources:

$$IPLR_{BSM} = IPLR_{link} + IPLR_{shaping} + IPLR_{congestion},$$

where:

- $Loss_{link}$ is the number of packets lost due to channel noise and residual errors;
- $Loss_{queuing}$ is the number packets lost due to traffic shaping;
- $Loss_{congestion}$ is the number packets lost due to congestion and ECN.

8.4.3.2.4 IP Error Ratio

IPER will be caused mainly by residual errors. Transmission errors will normally be corrected at the link layer (see clause 7.3.2.3.2). Some errors will be detected the packet's CRC and any residual transmission error will normally result in the packet being discarded hence IP packet loss.

8.4.4 End-to-end QoS budgets

When appropriate, end-to-end QoS measures will result in an end-to-end quality budget. To achieve the required end-to-end QoS the quality budgets must be allocated between source and destination. For the BSM it should include contributions from the SIAF but could also be limited to ingress SAP to egress SAP depending on the Service Level Agreement between the BSM operator and its clients. In an end-to-end scenario, it must be assumed that the contribution of each element in the end-to-end path is statistically independent from any other, in which case the budget can be computed in the following manner [17]:

$$\text{sum of all delays: } D_{tot} = D_1 + D_2 + \ldots.. D_n;$$

$$\text{total packet loss probability: } P_{tot} = 1 - [(1 - P_1) \times (1 - P_2) \times \ldots..(1 - P_n)]; \text{ and}$$

$$\text{Root Mean Square (RMS) total delay variation: } DV_{tot} = \sqrt{DV_1^2 + DV_2^2 + \ldots..DV_n^2},$$

where:

- D_n is the mean one-way delay of contributing element n;
- P_n is the packet loss probability of contributing element n;
- DV_n is the standard deviation of the delay variation of contributing element n.

8.4.5 Monitoring methods

These define how measurements are obtained using standard methods.

8.4.5.1 Polling

Polling means namely "ask" if a device is on. Traditional polling will use SNMP "Get" functions or ping functions to find out if a router is on. The traceroute function can also be used to see where a packet transited on the source to destination path.

For a BSM, a number of devices could answer to a polling message depending on its type. On the network side both the ST, the NCC or gateways that perform routing function should be able to reply to a polling message. On the spacecraft side, in the RSM family for example the onboard controller could be pinged or run a small version of SNMP to allow it to be managed (from the network point of view) using standard tools.

8.4.5.2 Probing

Probing sends a well-known stream from one host to another and then uses it to measure a number of performance parameters. This could be a powerful tool to ensure that the BSM is indeed fully operational as an IP subnetwork.

8.4.5.3 Traffic sampling

Traffic sampling, which can be done inside a router or a switch, means taking copies of some packets and verify source and destination, TTL etc. While it is not an essential part of performance monitoring it could be important in some security features and to establish statistics about flows that in turn could be used to establish traffic management parameters.

8.5 Quality rating

The TIPHON project has defined overall transmission quality Rating (R) as the full acoustic-to-acoustic (mouth to ear) quality, experienced by an average user, for a typical situation using a "standard" telephony handset. While this is only applicable to the voice services the idea of a "quality rating" for BSM services could lead to standard ways of evaluating end-to-end (SI-to-SI) performance over the BSM.

8.6 Network management

For a BSM the network management can be as complex as in any other broadband network. There is heritage in the FSAN approaches as well as in the current DSL and cable modem deployment. For the BSM itself the management will be located in the NCC but local functions related to usage accounting and billing could be located in the ST. More work is needed in the BSM network management and how performance and QoS management can be integrated to it.

8.6.1 SLA negotiations

The SLA negotiation will set the contract for the availability, latency and packet delivery of the offered service. There is one SLA per type of service (Internet, hosting, enterprise connectivity, etc.).

8.6.2 BSM-Specific Management Information Base (MIB)

The Management Information Base (MIB) contains data referring to managed objects organized in a hierarchical MIB tree. All objects are represented by MIB variables (numbers, lists, tables) which can be queried or modified. While the MIB goes beyond the scope of performance it does include performance management. Table 17 presents the attributes of some managed objects.

Table 17: Attributes of managed objects in a MIB

Defined attributes of managed objects	Description
Syntax	The type of data concerning a managed object.
Access	The type of access concerning the managed object.
Status	The availability of a managed object.
DesrcPart	A description in natural language.
ReferPart	Referenced documents.
IndexPart	MIB tables (defined as ASN.1 sequences) cannot be queried entirely; its entries have to be queried one at a time subsequently. Therefore, columns must be defined as index enabling access to single lines of the table.
DefValPart	Default value; it contains the initial values to be set in case of (re)start of the managed object.

It is usual in the Internet world to define Management Information bases for new technologies or protocols that impact network management. They can add attributes to existing MIB objects and add new objects that need to be managed in the new technologies. There is currently no BSM MIB (see recommended TSs).

8.7 BSM performance summary

Table 18 summarizes the role of each BSM subsystem in the management and measurement of QoS. As can be seen in the table each BSM element can and will pay a role in the setting, monitoring or measurement of QoS and performance parameters. For example, admission control is clearly distributed between the NCC, responsible for overall admission policy to onboard queues for local monitoring and the SI and SD part of the ST functions for local policies and monitoring. Table 18 links the actual function to the measured parameters and creates the template for the protocol manager described in the next clause.

Table 18: Summary of QoS/performance management by BSM subsystem

System component	Role	QoS function	Performance parameter
Customer network	IP packet generation Diffserv marking IP packet forwarding	Generates QoS parameter	Goodput Delay
SI	Convergence functions Segmentation/reassembly Queuing	Packet Marking ECN/EPD Pre-emption Flow/congestion control Admission control Performance Enhancing Proxies	Delay Delay variation Cell/packet loss
SD	BoD FEC Modulation Transmission	Admission control Power control	Delay BER Throughput Symbol rate Power level
Payload/bent pipe	Transmission	Power control	Delay Power level
Payload OBP	Demodulation Queuing Switching	Preemption Admission control Congestion control	Delay Delay variation Cell/packet loss BER Bit rate Symbol rate
Gateway/Satellite access server	Segmentation/reassembly Queuing FEC (De)Modulation	Packet Marking ECN/EPD Preemption Flow/congestion control Policy Management Performance Enhancing Proxies	Cell/packet loss Delay Delay variation BER Bit rate Symbol rate
NCC	Network Management	MIB Policy Management Security	Admission Control SIP PEP

9 BSM protocol manager

9.1 General description

From the previous clauses it is easily inferred that for maintaining QoS and evaluating performance of the BSM world in the Internet world, there is a need for some "manager". The protocol stack from the BSM drives the development of the Protocol Manager. The "manager" resides above the SAP and defines how IP protocols and packet markings are interpreted and transmitted through the BSM, which satellite independent (SI) protocols are used and how they in turn trigger the Satellite Dependent (SD) functions.

The Protocol Manager can be described as an "intelligent" traffic manager with packet classifier. It is a distributed process that manages traffic with reference to policies, admission control and other essential BSM metadata kept in an accessible and operator controlled database. It receives information from various interfaces and decides on the BSM protocol to trigger. At the convergence layer, it receives a packet and "classifies" it into some BSM functional or transport "bin". It will also interact with its peers, manage functional modules and ensure the integrity of the network by arbitrating between conflicting protocols.

The BSM Protocol Manager (BPM) must have the flexibility to support various types of BSM operators from a wholesale bandwidth provider to a network operator. It is located both at ingress and egress of the BSM and will have ST implementation as well as NCC implementations. This means that the capabilities of the BPM can range from offering:

- just connectivity - a layer 2 with or without priority;

- managed network services; and
- end-to-end and top to bottom capability.

Managing QoS can go from "do not care" (i.e. full transparency) to full capabilities for management, policing, marking etc. Hence the BPM architecture must be modular and easily upgradeable. Also, because of the nature of the BSM, the Protocol Manager will need to interact with different layers of the OSI stack: it will need to establish link layer negotiations to ensure link availability and integrity, it will have to translate RSVP messages into resource requests, it may need to throttle rates in times of fading etc. Finally, while the BPM could be designed as a QoS standalone in reality it will have to relate to other BSM management entities. Hence its implementation will have to rely on module and established module communications.

9.2 GSM heritage

The BPM has a lot of commonality with the QoS management functions for UMTS bearer service in the control and user plane. In UMTS and GPRS these include control functions for managing services, translate protocol primitives, perform admission control, and enforce policy [1]. These are in addition to mapping, classification, resource reservation and traffic shaping. In particular, at the convergence level GPRS uses packet information (DiffServ bits, IP protocol type, TCP/UDP port, IP address etc.) to assign is a Temporary Block Flow (TBF) with a Temporary Flow Identity (TFI) to some flow of multiplexed flow [1]. The radio dependent layer maintains temporary flow queues and allocates the TBF some radio resource on one or more channels. The assigned TFI is unique among concurrent TBFs in each direction and is used to uniquely identify a flow.

9.3 Architecture

An overview of the system is shown in figure 19. The BPM communicates at different levels of the BSM stack. While the middleware above IP is not fully in the scope of the BSM, the BPM will interact with specific middleware to establish transport level and application level PEPs, communicate with bandwidth brokers and potentially with service discovery and security/authentication functions. The manager interacts directly with IP protocols, including MPLS for route discovery and Intserv, DiffServ models. At the convergence layer the BMP sets queuing policies and SI adaptation functions (SAIF). If the BSM only acts as a bridge then the Protocol manager can interact with Ethernet protocols to establish virtual LANs (VLANs) and authenticate source-destination pairs. In this model the BMP does not interact directly with the SD part of the BSM stack. All SD functions are controlled and negotiated by SI proxies and indirectly via the BMP. The goal of the BMP is to interwork across all BSMs.

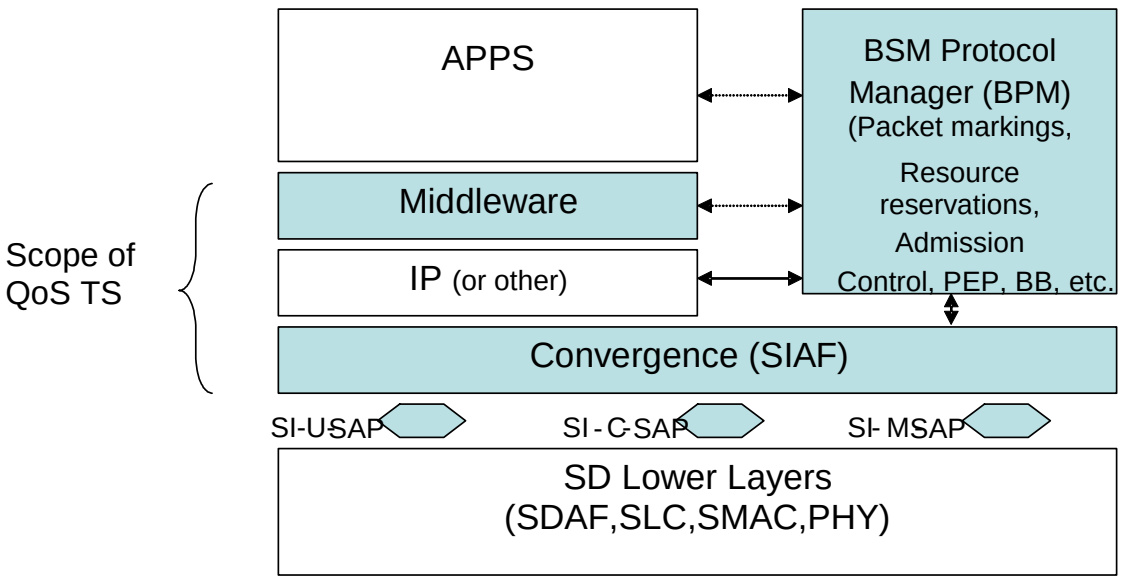


Figure 19: Protocol manager - System architecture

9.4 Description

A detailed view of the BPM software is available in figure 20. It uses a client-server model with a modular approach to the development of specific functions. Initial descriptions are available in the next clauses.

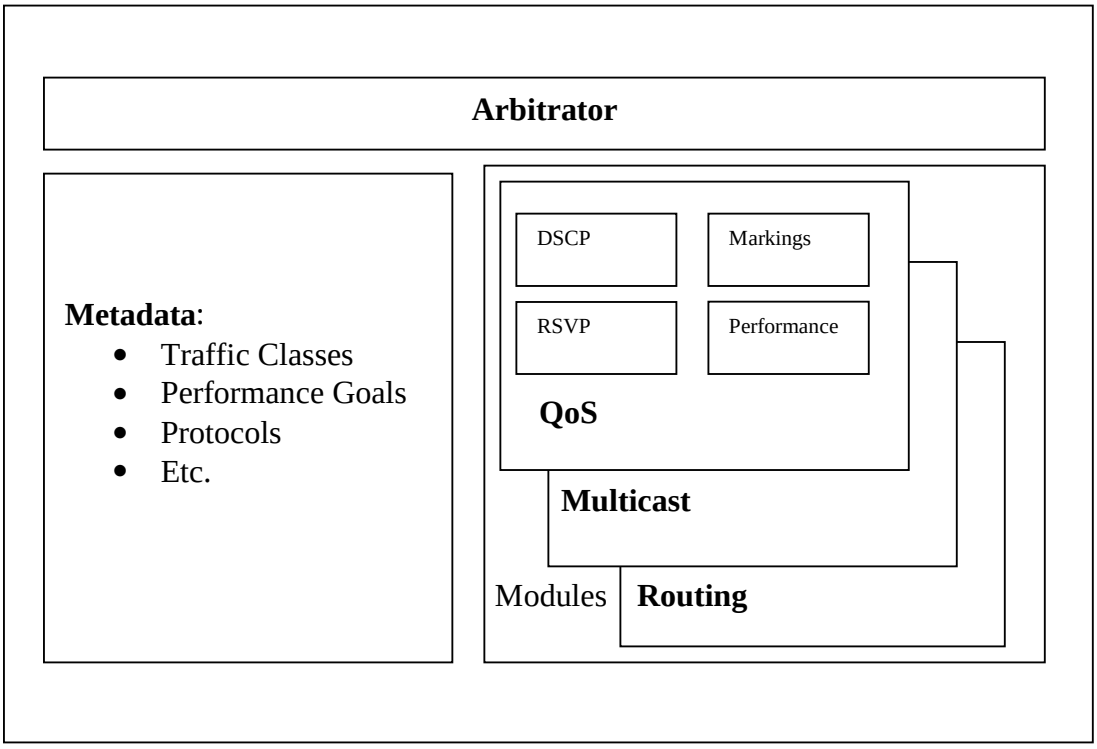


Figure 20: BMP software overview

9.4.1 Arbitrator

The Arbitrator enables IP to BSM event modelling and interpretation. It supports a central database of metadata describing IP (or other protocols) and traffic characteristics and manages the different modules. The metadata, in essence a Management Information Base (MIB), enables API translation from the requesting application to the BSM modules APIs. This information will contain the list of supported IP protocols and their version, the list of supported SI functions and other specific information that will allow an application to receive appropriate service over the BSM. It is not necessary for the arbitrator to use IP protocols to communicate with its peer and other proprietary or standard protocols (from UMTS or GPRS) could be used.

9.4.2 Metadata

Table 19 illustrates the type of metadata that the arbitrator will use to manage the QoS protocols over the BSM.

9.4.3 Modules

The Module Framework enables modular implementation and SI abstraction of basic BSM functionality. Each module can specify and provide a native API as a library. The states of the resource a single module manages are kept in a single location but the set of modules can be located in many servers across the BSM (even across the Internet). Modules can be dependant on each other and when in conflict will report back to the Arbitrator for resolution.

9.4.3.1 QoS and performance modules

For QoS the BPM performs a number of different functions: signalling to and from the BSM, protocol and requirement translation, packet marking, statistics gathering and performance reporting. The BPM also has an important role in the admission of sessions in the BSM and in the triggering of mechanism for flow and congestion control especially when congestion is due to a link failure. For QoS management it also handles the Intserv signalling, Diffserv markings and performance management.

9.4.3.1.1 Admission/flow/congestion control

Admission, flow and congestion control are essential SIAF. As such the BPM should be able to communicate with and set parameters or trigger drop mechanisms. This module could be fairly transparent to existing SIAFs.

9.4.3.1.2 RSVP and Intserv

In the Intserv model, the BMP can act directly on the RSVP packets or being provisioned by a COPS server. In the first case, it is the BPM that will receive the RSVP messages and respond to them. It will also translate flowspecs into SI parameters, link flow ids to internal BSM ids and send the RSVP message to the next router on the path. In particular by triggering BoD SIAF functions the BPM will ensure there is enough bandwidth for the required flow. In addition the BPM should manage signalling queues and ensure that signalling messages do not become stale. In the second case the BMP still manages the BSM resources but does it indirectly and does not have to maintain RSVP state information.

For MPLS, the RVSP-TE messages should be handled the same way. If the BMP is in direct interaction mode, the "state" will become the label. Finally, SIP signalling should be transparent to the BSM with the call proxy initiating the reservation when appropriate.

9.4.3.1.3 Diffserv - Markings and negotiations

For DiffServ, the role of the BPM is to map DS from attached networks into BSM priorities and negotiate values when appropriate and mark packets in and out of the BSM. The role of the BPM is to define the priority (and UDTS), based on available packet information, thus translating from DS to BSM priorities. The UDTS and priority are set by inspection of DS field. The BPM also ensures that the overall management structure needed for the BSM Diffserv per hop behaviour is performing properly.

9.4.3.2 Performance/Availability

Based on the performance goals, the BPM will lower layer capabilities to ensure the BSM is operating at nominal performance. No IP protocol should have to decide on modulation or coding. The BPM will contain a query module to the SIAF that in turn will get the right information from the SDAF to ensure that the connection is error free or at least error predictable and within the contract established with the BSM customers. When it does not the BPM can set link congestion and invoke flow control mechanisms. The SI-SAP accommodates modulation and coding variation purely by flow control and there is no need to propagate link layer characteristics above SI-SAP; in essence the BPM needs to know what is wrong and ask for correction.

The BPM may also request from a suite of other available link layer services such as compression, encryption and so on. Joint Network/Link mechanisms can only exist within the BPM and once a DS class has been established the BPM will support it by requesting a change to modulation and coding when appropriate.

Table 19: QoS metadata (example)

Database entries	Description	Parameters	Notes
QoS service class	Describes the end-to-end class of the BSM bearer service.	TBD/will include a number of QoS class and a best effort class.	Parameters specifying the BSM QoS Class; suggested as a potential TS.
Codec type and packetization (optional)	Describes the Codec type used on a bearer and the way the media is packetized.	Codec Type (Optionally a list of possible codecs).	Codec Identifier including any relevant codec parameters, e.g. version number, sampling rate, etc.
		Frames per packet (Optionally a list when codec lists are specified).	Number of frames per packet.
Transport QoS parameters	Specifies the QoS characteristics of the service or flow.	Maximum Delay	The maximum delay permitted over either the BSM only or the end-to-end budget.
		Maximum Packet Delay Variation	The maximum packet delay variation permitted over either the BSM only or the end-to-end budget.
		Maximum Mean Packet Loss	The maximum mean packet loss permitted over either the BSM only or the end-to-end budget.
Traffic descriptor	Characterizes the resource requirements of a flow.	Peak Bit	Maximum bit rate (bit/s) of a flow.
		Maximum Packet Size	Maximum size of the packets.
Source and destination IDs	Specifies the identity of the source and destination.	Source ID	The identity of the source (Ethernet MAC address, IP address, SIP URI).
		Destination ID	The identity of the destination (Ethernet MAC address, IP address, SIP URI).
Application data transport protocol	Specifies the application data transport protocol.	Protocol ID	Identifier of the application data transport protocol used by the bearer. RTP or RTSP etc.
Packet transport protocol	Specifies the packet transport protocol.	Protocol ID	Identifier of the packet transport protocol used in the transport flow. Typically UDP or TCP.
QoS policy	Describes the policy determining the user's entitlement to QoS Service Class.	Token bucket depth Congestion control mechanisms, etc.	The policies implemented to control traffic ingress and egress in the BSM.
QoS mechanism	Describes the mechanism used in the Transport Plane.	Type	None, RSVP/Intserv, DiffServ or MPLS.
		Mechanism specific parameters	TBD
		Authorization Token	TBD

10 Recommended Specifications to be produced by ETSI

10.1 Common characteristics across all TSs

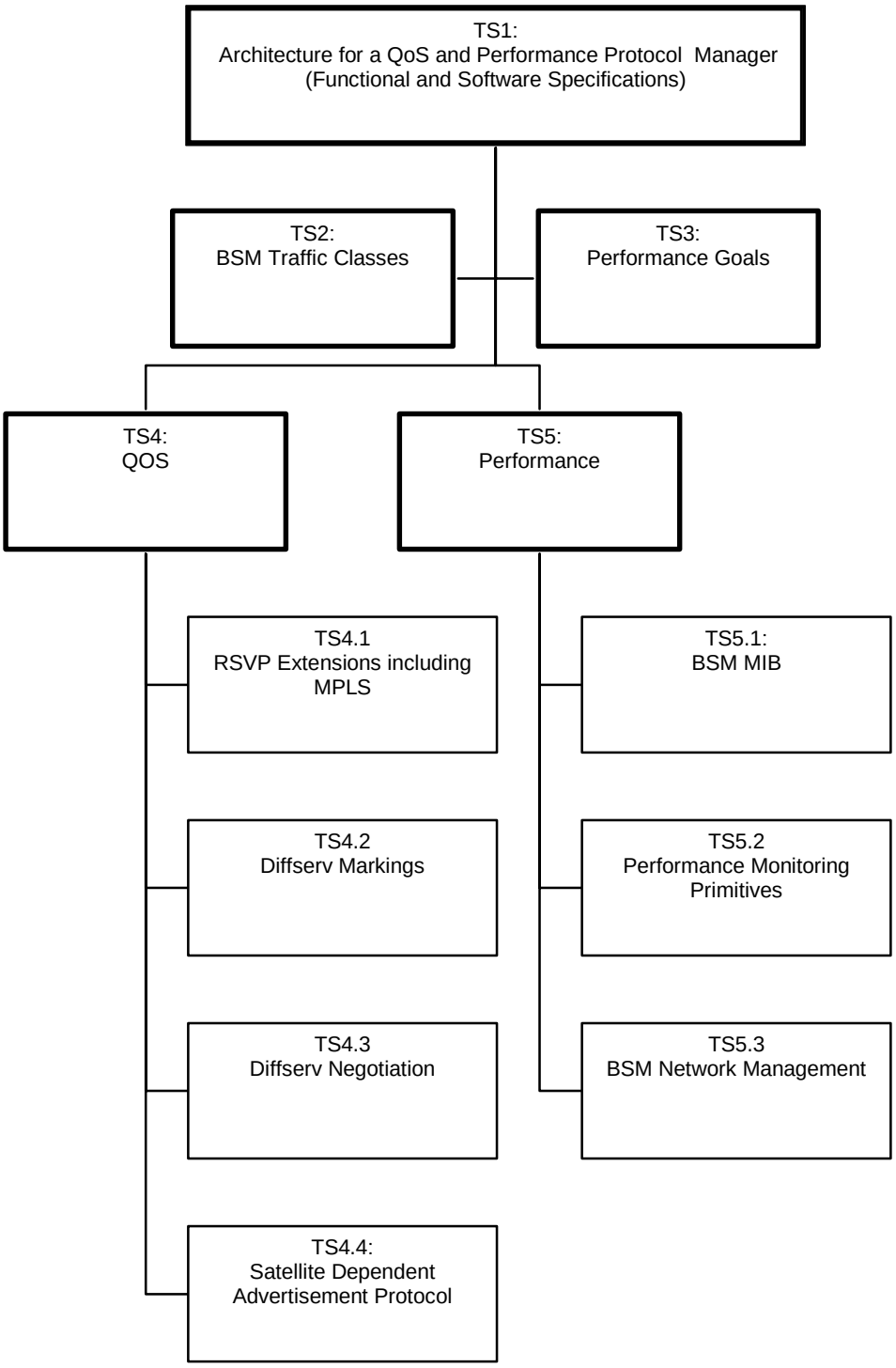


Figure 21: Recommended Technical Specifications

Figure 21 presents the structure of the recommended TSs. As can be seen in figure 21 those are separated in 2 Categories, QoS and Management. Traffic Classes and Performance Goals are added higher-level modules. All TSs are modules of the main TS: the protocol manager for QoS and Performance.

All recommended TSs share the following characteristics, namely:

- the use of open specifications: none of the proposed TSs will be proposing a specification that is not part of public knowledge and any software implementation will use open software and operating system;
- all specifications will directly build on existing link layer interface primitives to ensure continuity;
- all specifications should be located in the satellite independent layers and should be independent of the specifics of the satellite dependent lower layers; while some QoS parameters may depend on specific implementation the protocols themselves should be applicable to any family of lower layers;
- all specifications will interwork with IP functions; and
- all specifications will interwork with application layers above it using an open API; this includes network management software.

10.2 TS1: Architecture

The protocol manager was described in details in clause 9.

10.3 TS2 and TS3: Generic TSs

Two top-level TSs are proposed to deal with generic QoS and performance requirements in the BSM:

- TS2: a BSM specific set of traffic classes (based on ITU-T, 3GPP and TIPHON) defined and leading to achievable goals in term of delay, jitter and loss. A preemption class to allow time-stamped messages to get fast access to the BSM may be considered; and
- TS3: a BSM specific set of network performance parameter based on measurable parameters at the ST, the NCC/gateway and the satellite payload; this can be based on ITU recommendations but also include BSM specific parameters related to air interface management and multicasting.

They are summarized in table 20.

Table 20: Summary of generic Specifications

Specification number	QoS management function	Specification	Recommended action
TS2	Traffic classes	Delay Jitter Throughput Goodput Bandwidth on Demand Pre-emption	Specify a BSM specific set of traffic classes
TS3	Performance parameters	Delay Jitter Throughput Goodput Loss Availability	Specify a BSM specific set of performance parameters

10.4 TS4.x: QoS specific TSs

Technical specifications that are specific to QoS include:

- TS4: BSM specific functions for QoS management in Intserv and Diffserv models:
- TS4.1: a set of RSVP-like primitives and proxy manager using the current air interface primitives to identify RSVP messages and request and reserve bandwidth across the BSM; this is particularly needed in the access network scenario where RSVP has the biggest chance of being deployed; this TS also includes how the BSM defines the MPLS labelled paths that are discovered by RSVP-TE; this TS could include COPS interactions;
- TS4.2: a set of QoS primitives and proxy manager to be located at the ingress of the BSM to identify and map Diffserv markings to BSM traffic classes (and the inverse at the egress); this is for the content delivery scenario and when the BSM will be involved in interdomain communications;
- TS4.3: a middleware component and QoS manager in the NCC or gateway to negotiate and manage codepoint values with attached networks; this is complementary to the previous recommendation and also necessary in interdomain communications; and
- TS4.4: the development of a set of "Network Status Advertisement Protocols (NSAPs)" to advertise the status of the BSM to the network (interlayer processes); this in turn can be used to police and shape traffic and set congestion avoidance parameter across the BSM and its attached networks.

A short description is available in table 21.

Table 21: Summary of QoS Specifications

Specification number	QoS management function	Specification	Recommended action
TS4	Top level description of QoS management		
TS4.1	RSVP extensions	Primitives for Flowspec MPLS Priority Pre-emption	Specify primitives and manager for RSVP over BSM
TS4.2	Diffserv markings	Primitives for Packet Markings DSCP Congestion feedback RED	Specify primitives and for Diffserv over BSM
TS4.3	Diffserv negotiations	DSCP management	Manages DSCP across BSM boundaries
TS4.4	NSAP	Interlayer signalling	Specify a protocol to signal BSM status to attached networks

10.5 TS5.x: Performance specific TSs

Technical specifications that are specific to Availability and Performance include:

- TS5: s series of performance management functions to manage BSM performance;
- TS5.1: the development of a BSM specific Management Information Base; this would be based on the known MIBS for other technologies and would standardize not only the performance of the BSM, but BSM semantics and points of measurements; it will also help to include the BSM into larger management bases;
- TS5.2: a set of performance primitives based on SMNPv2 semantics to interrogate the BSM subsystem for specific performance parameters; this would be used by local or network managers to establish the "health" of the BSM; there is heritage in this in PC technologies and cable and satellite set-top boxes; and
- TS5.3: the development of BSM specific management software requirements to integrate into network management software; this is a large task but needed to ensure that the BSM becomes only "another network".

These TSs are summarized in table 22.

Table 22: Summary of performance Specifications

Specification number	Performance management function	Specification	Recommended action
TS5	Top level description of performance issues		
TS5.1	BSM MIB	Definition of performance elements to allow BSM management	Link to other technologies
TS5.2	Performance primitives	Definition of how to measure BSM performance	Specify a BSM specific set of performance primitives
TS5.3	BSM network management	Performance and network management functions	Develop software specifications for BSM performance management that integrate to COTS network management software

Annex A:
IP QoS standardization

Table A.1 lists most of the current standardization groups dealing with QoS.

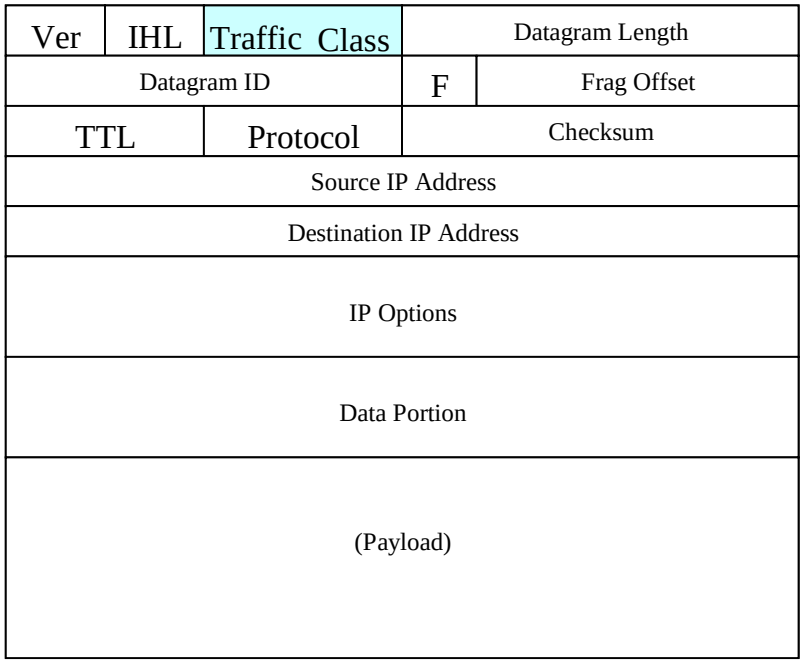
Table A.1: Standardization work on QoS

Standards body	Working Group	IP QoS impact	Notes
Internet Engineering Task Force (IETF)	Intserv	Flow based model, RSVP signalling	
	Diffserv	Packet markings, QoS management	
	PILC	Suggest strategies for over links that could offer challenges	
	tcpsat	Mechanisms	Work completed
	NSIS	QoS signalling	
	ippm	Performance metrics for QoS	
	bmwg	Benchmarking Methodology	
	rap	Resource Allocation Protocol QoS routing and traffic management	COPS
	MPLS	IP over DVB issues	
	ip-dvb	Trigger mechanisms for wireless subnets	Proposed WG
	trigtran		Proposed WG
International Telecommunications Union Telecommunications Standardization (ITU-T)	Study Group 2: Operational aspects of service provision, networks and performance	QoS aspects and performance	
	Study Group 12: End-to-end transmission performance of networks and terminals	Metrics and performance	
	Study Group 13: Multi-protocol and IP-based networks and their internetworking	IP QoS and its measurement	
	Study Group 16: Optical and other transport networks	Multimedia services, systems and terminals	
Radiocommunications Standardization (ITU-R)	Study Group 4 (Working Party 4B) Systems, performance, availability and maintenance	Link layer aspects	
	Study Group 6 Radio communication broadcasting		

Standards body	Working Group	IP QoS impact	Notes
European Telecommunications Standards Institute (ETSI)	TIPHON SPAN	Voice-centric model System Signalling - link to QoS signalling	
3GPP	UMTS GPRS	Large implication in QoS - terminal level issues	
IEEE	802.1p	Adds 8 levels of priority	Protocol Independent
Cable Laboratories Inc. (CableLabs)	DOCSIS PacketCable	Defines QoS for data over Cable RVSP over DOCSIS	 uses Dynamic QoS to renegotiate parameters during a session
Digital Video Broadcasting (DVB)	DVB IPI	Work in Progress	May not develop new protocols
Telecommunication Industry Association (TIA)	WG 34-1	ATM over satellite	
ATM Forum	S-ATM	ATM over satellite	

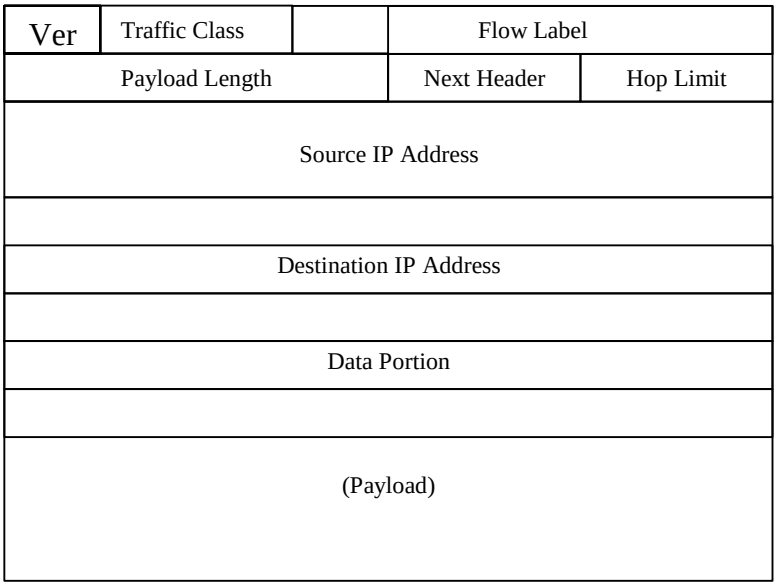
Annex B:
Internet packet formats

Every packet has at least two parts. First, a fixed length HeaDeR (HDR) contains the packet specifics (addresses, QoS, etc.). Then a variable length payload contains other protocol information, application data and potentially error protection codes. Header information allows to forward the packet and under which conditions.



VER VERsion.
IHL IP Header Length.
F Flags.
TTL Time To Live.

Figure B.1: IPv4 packet format



NOTE: Flow label: identify a stream of packets with same SA and DA.

Figure B.2: IPv6 packet format

Annex C:
Lightweight Interlayer Signalling Protocol (LISP)

Transmit link layer status (BER, availability, etc.) as:

- ICMP command to control the source.
- Input to the "path" computation in OSPF to avoid routing to a link with problems.

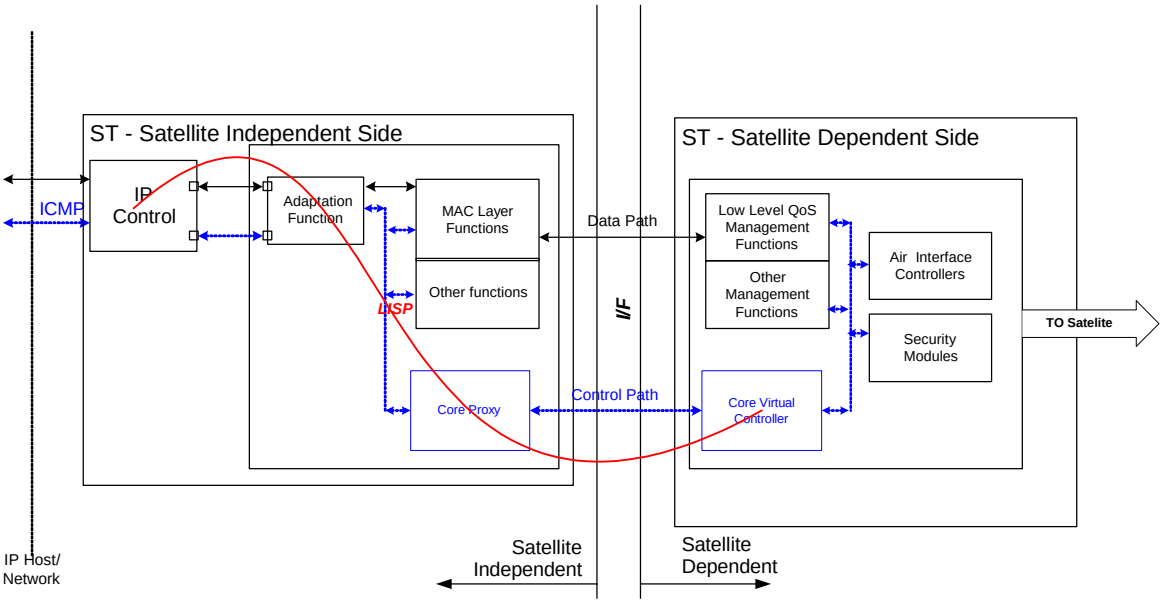


Figure C.1: LISP overview

Annex D:
Performance summary

Parameter	Description	Test metric	Comment	BSM measure
One way transmission time	Time in milliseconds between the emission of a signal and the time it is received, includes delays due to equipment processing as well as propagation delay.	Mean packet transmission time/ms; Minimum and maximum packet transmission times/ms.	Needs synchronized boxes.	Ingress SAP to egress SAP.
Roundtrip transmission time	Time in milliseconds for a packet to be transmitted from host A and received at host B and to be re-transmitted from host B and received back at host A.	Mean roundtrip packet transmission time/ms; Minimum and maximum packet transmission times/ms.	The reflection of a packet for roundtrip measurement should be at the protocol layer that the measurement is addressing.	Ingress SAP to egress SAP.
2 Point packet delay variation	PDV is the difference between upper and lower percentiles on the packet delay distribution. 2pt PDV uses 2 monitoring points. The measurement uses the difference between the inter-packet sending and inter-packet arrival times.	2pt packet delay variation/ms.	Measurement requires two synchronized test boxes.	Ingress SAP to egress SAP.
1 Point packet delay variation	PDV is the difference between upper and lower percentiles on the packet delay distribution. 1pt PDV uses only 1 monitoring point. The measurement is based on the inter-packet arrival times.	1pt packet delay variation/ms.	Measurement requires a single test box and therefore no synchronization.	
Network packet loss	Percentage of packets lost at an IP test point; this metric does not include any losses due to the end-terminal equipment.	% network packet loss; Total number of lost packets.	None.	Could include some of the SIAF losses (queuing losses).
Effective packet loss	Percentage of packets lost as measured at the input of the speech codec, affecting the speech coder performance.	% network packet loss; Total number of lost packets; Packet loss distribution.	None.	Voice only. Could be extended to video.
Packet errors	Packets that fail the CRC when received at an IP test point.	Percentage of errored packets; Total number of errored packets.	Errors in a data packet will normally result in a packet being dropped by the layer 2 protocols However CRC can sometimes fail and this can be monitored using the test tools available.	This is above the link detection of errors. The whole BSM packet error should include both contributions.
Mis-sequenced packets	Out of sequence packets at the receiving IP test point	Number of mis-sequenced packets.	A large number of mis-sequenced packets may indicate a congested network or that load balancing is in use.	Ingress SI to egress SI.

Annex E: Bibliography

Afonso, M., Santos, A. and Freitas, V.: "QoS in web caching", in Proceedings of the Third International WWW Caching Workshop, Manchester, England, June 1998.

Bolla, R. et al.: "Bandwidth Allocation in a Multiservice Satellite Network Based on Long Term Weather Forecast Scenarios", Computer Communication Journal, vol. 25, 2002, pp. 1037-1046.

Choi, S. and Shin, K.G.: "An Uplink CDMA System Architecture with Diverse QoS Guarantees for Heterogeneous Traffic", IEEE/ACM Transactions on Networking, vol. 7. no. 5, October 1999.

Clausen, H.D., Linder, H. and Mirlacher, T.: "Multicast Cache Updating via Satellite", IEEE Workshop on Computer Communications, Mississippi, Oct. 1998.

Davie, B. and Rechter, Y. MPLS: Technology and Applications, Morgan Kaufmann Publishers, 2000.

ETSI TR 101 374-1 (V1.2.1): "Satellite Earth Stations and Systems (SES); Broadband satellite multimedia; Part 1: Survey on standardization objectives".

ETSI TR 101 374-2 (V1.1.1): "Satellite Earth Stations and Systems (SES); Broadband satellite multimedia; Part 2: Scenario for standardization".

European Union IST Programs: "IP ConferEncing with Broadband multimedia over Geostationary Satellites (ICEBERGS)", 2002.

Fu, A, Modiano E. and Tsitsiklis, J.: "Optimal Energy Allocation and Admission Control for Communications Satellites", IEEE INFOCOM 2002, New York, June, 2002.

Hung, A., Montpetit M.J., Kesidis, G. and Takats, P.: "A Framework for ATM via Satellite", Proceedings of Globecom, London, Nov. 1996

Internet draft-demeer-nsis-analysis-02, de Meer, H. ed.: "Analysis of Existing QoS Solutions", June 2002.

Internet draft Fu, draft-fu-rsvp-multicast-analysis-01, Fu, X., Kappler, C. and Tschofenig, H.: "Analysis on RSVP Regarding Multicast", October 2002.

Internet draft ASYM, draft-pilc-asym-07, Balakrishnan, H. ed.: "TCP Performance Implications of Network Path Asymmetry v. 7", November 2001.

Internet draft DCCP, draft-ietf-dcc-spec-00, Kohler, E. et al., "Datagram Congestion Control Protocol", October 2002.

Internet draft Martini, draft-martini-ethernet-encap-mpls-01: "Encapsulation Methods for Transport of Ethernet Frames over IP and MPLS Networks", July 2002.

Internet draft PWE3 draft-pate-pwe3-framework-03, Pate P. ed.: "Framework for Pseudo-Wire Emulation Edge to Edge (PWE3)", January 2002.

Internet draft LINK, Internet draft-pilc-link-design-11, Karn, P. ed: "Advice for Internet Sub network Designers v. 11", May 2002.

Internet draft TRIGTRAN, draft-dawkins-trigtran-probstmt-00, Dawkins, S. Williams, C.E, Yegin, A.: "Problem Statement for Triggers for Transport (TRIGTRAN)", October 2002.

Karagiannis, G. et al.: "Resource Management in Diffserv (RMD): A Functionality and Performance Behaviour Overview", Proceedings of Protocols for High-Speed Networks 2002, pp. 17-34.

Keshav, S.: "An Engineering Approach to Computer Networking", Addison Wesley, 1997.

Kuiper, F. at al.: "An Overview of Constraint-based Path Selection Algorithms for QoS Routing", IEEE Communications Magazine, December 2002.

Leboeuf, E., Rosenberg C. and Montpetit, M.J.: "Availability as a QoS Parameter in Dynamic Physical Layer Systems: An Application to Satellite Networks", Submitter to the IEEE Journal on Selected Areas in Communications, 2002.

Ma, Q. and P. Steenkiste: "On Path Selection for Traffic with Bandwidth Guarantees", Proc. 5th IEEE International Conference on Network Protocols, Oct. 1997.

Metrtzanis, I. et al.: "Protocol architectures for satellite ATM broadband networks", IEEE Communications Magazine, March 1999.

Mehdi, D.: "QoS Routing Computation with Path Caching: A Framework and Network Performance", IEEE Communications Magazine, December 2002.

Ors, T. and Rosenberg, C.: "Providing IP QoS over GEO Satellite Systems Using MPLS", International Journal of Satellite Communications, Volume 19, Issue 5, 2001, pp. 443-461.

RFC 1157 (1990): "Simple Network Management Protocol".

RFC 1212 (1991): "Concise MIB Definitions".

RFC 1323 (1992): "TCP Extensions for High Performance".

RFC 1889 (1996): "RTP: A Transport Protocol for Real-Time Applications".

RFC 2326 (1998): "Real Time Steaming Protocol (RTSP)".

RFC 2327 (1998): "SDP: Session Description Protocol".

RFC 2544 (1999): "Benchmarking Methodology for Network Interconnect Devices".

Wang, Z. Internet QoS: "Architectures and Mechanisms for Quality of Service", Morgan Kaufman, 2001.

List of figures

List of tables

History

Document history		
V1.1.1	July 2003	Publication