

Consultative Committee for Space Data Systems

**RESEARCH AND DEVELOPMENT FOR
SPACE DATA SYSTEM STANDARDS**

Next Generation Space Internet (NGSI)—End-to-End Resource Provisioning for Orbiting Missions

CCSDS 732.5-O-1

EXPERIMENTAL SPECIFICATION

April 2003



AUTHORITY

Issue:	Current Issue
Date:	April 2003
Location:	Matera, Italy

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in the *Procedures Manual for the Consultative Committee for Space Data Systems*.

This document is published and maintained by:

CCSDS Secretariat
Office of Space Communication (Code M-3)
National Aeronautics and Space Administration
Washington, DC 20546, USA

PREFACE

This document is a CCSDS Experimental Specification. Its Experimental status indicates that it is part of a research or development effort based on prospective requirements, and as such it is not considered a Standards Track document. Experimental Specifications are intended to demonstrate technical feasibility in anticipation of a ‘hard’ requirement that has not yet emerged. Experimental work may be rapidly transferred onto the Standards Track should a hard requirement emerge in the future.

FOREWORD

This Experimental Specification describes end-to-end resource provisioning for orbiting missions within the proposed Next Generation Space Internet (NGSI) architecture.

Through the process of normal evolution, it is expected that expansion, deletion, or modification to this document may occur. This Experimental Specification is therefore subject to CCSDS document management and change control procedures which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

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

Questions relating to the contents or status of this report should be addressed to the CCSDS Secretariat at the address on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- National Aeronautics and Space Administration (NASA)/USA.
- National Space Development Agency of Japan (NASDA)/Japan.
- Russian Space Agency (RSA)/Russian Federation.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Communications Research Centre (CRC)/Canada.
- Communications Research Laboratory (CRL)/Japan.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Federal Service of Scientific, Technical & Cultural Affairs (FSST&CA)/Belgium.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space and Astronautical Science (ISAS)/Japan.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Program Office (NSPO)/Taipei.
- Space & Upper Atmosphere Research Commission/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 732.5-O-1	Next Generation Space Internet— End-to-End Resource Provisioning for Orbiting Missions	April 2003	Current Issue

CONTENTS

<u>Section</u>	<u>Page</u>
1 INTRODUCTION.....	1-1
1.1 PURPOSE.....	1-1
1.2 SCOPE.....	1-1
1.3 REFERENCES.....	1-1
2 OVERVIEW.....	2-1
3 RSVP IN THE NGSI ARCHITECTURE.....	3-1
3.1 OVERVIEW OF RSVP.....	3-1
3.2 RSVP EXTENSIONS FOR IPSEC.....	3-1
3.3 RSVP EXTENSIONS FOR IP MOBILITY.....	3-1
3.4 RSVP AND PROTOCOL TRANSLATING GATEWAYS.....	3-2
4 CONCLUSIONS.....	4-1
ANNEX A ABBREVIATIONS AND ACRONYMS.....	A-1
ANNEX B INFORMATIVE REFERENCES.....	B-1

Figure

2-1 NGSI Architecture.....	2-1
3-1 RSVP Interactions.....	3-1
3-2 ORIG_IPPROTO Object.....	3-3

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Experimental Specification is to define the protocols necessary for end-to-end network-level resource reservation in space communication environments. In particular, this document describes how the Resource Reservation Protocol (RSVP) should be extended to function in conjunction with the end-to-end security services described in reference [1] and the spacecraft Internet Protocol (IP) mobility services described in reference [2].

1.2 SCOPE

This Experimental Specification addresses end-to-end signaling of resource requirements. Mechanisms to support the allocation and management of the resources at the network layer and below are assumed. For example, reference [4] gives an extensive list of routers and end host implementations that are RSVP-compliant.

This Experimental Specification assumes an architecture involving end-to-end communications between Internet-based hosts and orbiting assets.

1.3 REFERENCES

The following documents are referenced in this Experimental Specification. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Experimental Specification are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS Recommendations.

- [1] *Next Generation Space Internet (NGSI)—End-to-End Security for Space Mission Communications*. Experimental Specification for Space Data System Standards, CCSDS 733.5-O-1. Experimental Specification. Issue 1. Washington, D.C.: CCSDS, April 2003.
- [2] *Next Generation Space Internet (NGSI)—Supporting Spacecraft IP Mobility*. Experimental Specification for Space Data System Standards, CCSDS 733.0-O-1. Experimental Specification. Issue 1. Washington, D.C.: CCSDS, April 2003.
- [3] *Next Generation Space Internet (NGSI)*. Report Concerning Space Data System Standards, CCSDS 733.0-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, April 2003.
- [4] Gaines, G. and M. Festa. *A Survey of RSVP/QoS Implementations*. Update 2. July 1999. http://www.isi.edu/rsvp/DOCUMENTS/ietf_rsvp-qos_survey_02.txt

CCSDS EXPERIMENTAL SPECIFICATION FOR NEXT GENERATION SPACE INTERNET
(NGSI)—END-TO-END RESOURCE PROVISIONING FOR ORBITING MISSIONS

- [5] Braden, R., Clark, D. and S. Shenker. *Integrated Services in the Internet Architecture: an Overview*. RFC 1633, June 1994.
- [6] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin. *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*. RFC 2205, September 1997.
- [7] Berger, L., and T. O'Malley. *RSVP Extensions for IPSEC Data Flows*. RFC 2207, September 1997.
- [8] Wroclawski, J. *The Use of RSVP with IETF Integrated Services*. RFC 2210, September 1997.
- [9] Terzis, A., Krawczyk, J., Wroclawski, J., and L. Zhang. *RSVP Operation Over IP Tunnels*. RFC 2746, January 2000.

2 OVERVIEW

This Experimental Specification describes the protocols and extensions needed to support end-to-end signaling of resource requirements. It assumes an architecture where end-to-end communications paths (i.e., from spacecraft to Internet-based host) exist.

The reference NGSI architecture, shown in figure 2-1, includes advanced Internet Protocol (IP) networking technologies such as MobileIP, Internet Protocol Security (IPSEC), Space Communications Protocol Specification-Security Protocol (SCPS-SP), and protocol translating proxies.

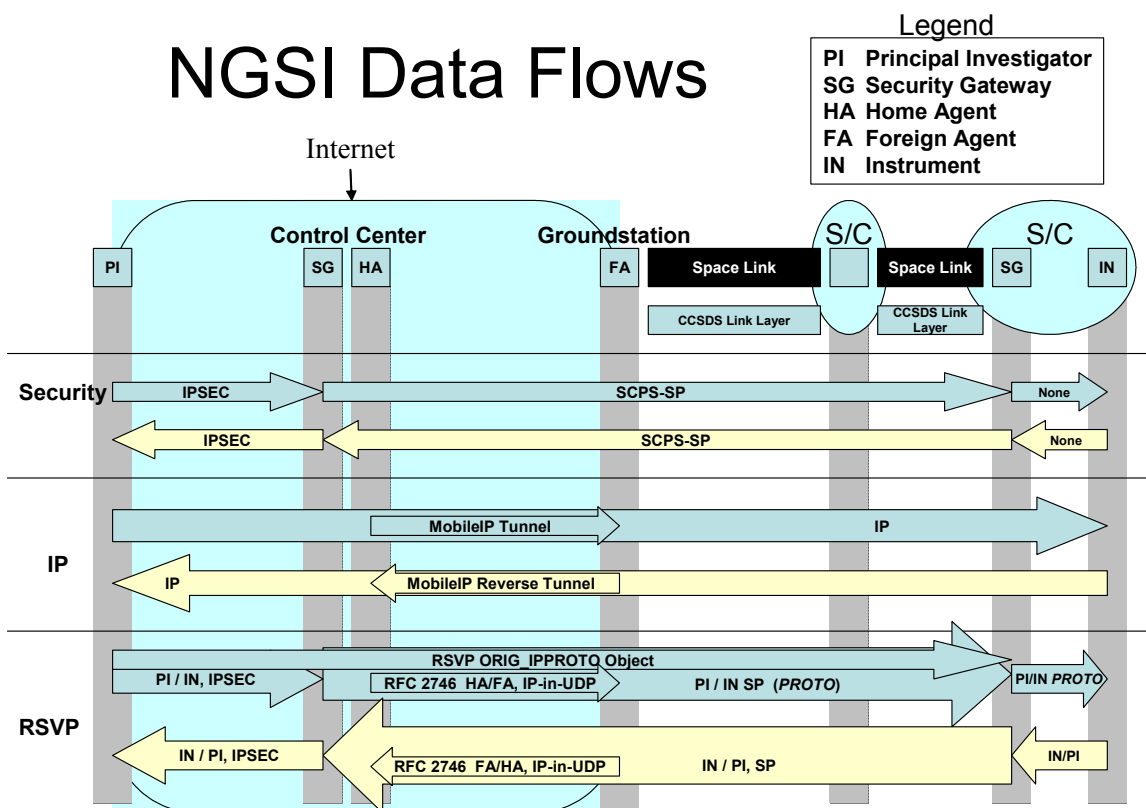


Figure 2-1: NGSI Architecture

For a discussion of the architectural and deployment issues related to RSVP, see reference [3]. The different slices of figure 2-1 represent different views of the network path, as seen by security, IP, and RSVP. For the RSVP slice, the notations in the arrows (e.g., PI/IN, IPSEC) refer to the source and destination IP addresses and IPPROTO number of packets for which resources are reserved at that point. Thus as far as RSVP is concerned, a reservation for data flowing from PI to space in the portion of the network path between the control center and the ground station would carry an RSVP SESSION object reserving resources for packet from the home agent to the foreign agent of type Universal Datagram Protocol (UDP) (IP-in-UDP encapsulation).

3 RSVP IN THE NGSI ARCHITECTURE

3.1 OVERVIEW OF RSVP

The Resource Reservation Protocol (RSVP) (references [5] through [8]) provides a mechanism that allows hosts to signal resource usage requests along network paths. RSVP can be used in conjunction with quality of service control mechanisms to provide improved Quality of Service (QOS) to applications (reference [8]).

With RSVP, special daemons are present in the source, routers, and destination that make up a communications path. Data senders send RSVP PATH messages to destinations, which respond with RSVP RESV (reservation) messages. The RSVP Daemons in intermediate routers react to the PATH and RESV messages by communicating with other router elements to allocate buffer spaces and link bandwidth to the flow. Figure 3-1 shows the elements and data flows for RSVP resource reservation.

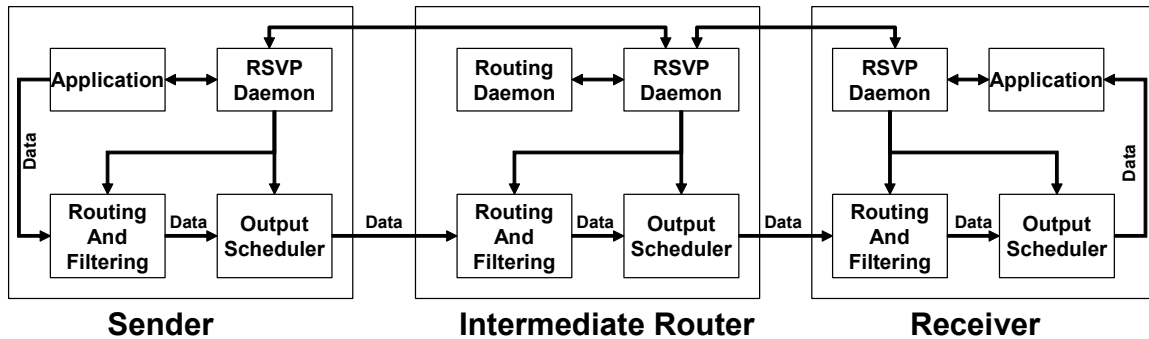


Figure 3-1: RSVP Interactions

3.2 RSVP EXTENSIONS FOR IPSEC

If Next Generation Space Internet (NGSI) security gateways are used, an NGSI RSVP must implement the following Internet Engineering Task Force (IETF)-defined extension:

- RSVP Extensions for IPSEC Data Flows (RFC 2207, reference [5]) specifies the use of Generic Port Identifiers (GPIs) to differentiate between IPSEC-protected flows.

NOTE – SCPS-SP does not contain an analog to IPSEC's security parameter index. This means that RSVP cannot differentiate among multiple SCPS-SP flows. For the NGSI reference architecture depicted in figure 2-1 this is not a problem, as the SCPS-SP flows in the Internet are themselves encapsulated by MobileIP.

3.3 RSVP EXTENSIONS FOR IP MOBILITY

If IP Mobility is used, an NGSI RSVP must implement the following IETF-defined extension:

- RSVP Operation Over IP Tunnels (RFC 2746, reference [9]) addresses modifications to RSVP daemons to support operation with IP-in-IP and IP-in-UDP tunneling.

3.4 RSVP AND PROTOCOL TRANSLATING GATEWAYS

3.4.1 IPPROTO FIELD

While the NGSI security gateways do not modify the source and destination addresses of packets traversing them (as MobileIP tunnels do), they do change the IPPROTO field of the packets that flow through them. For example, packets entering the upstream gateway with an IPPROTO field of 50 (IPSEC Encapsulating Security Payload) exit with an IPPROTO field of 99 (Private Security, used for SCPS-SP). Thus the RSVP SESSION objects associated with these flows must be modified so that they leave the gateway with the appropriate protocol number (99 in this case).

At the downstream security gateway, the RSVP SESSION object must be modified again to reflect the IP protocol of outbound packets. For example, if the original encrypted traffic entering the upstream gateway was UDP, the IPPROTO for RSVP SESSION objects leaving the downstream gateway needs to be decimal 17. Note also that these modifications to the SESSION objects must be made without examining the actual data packets. That is, one cannot simply examine the IPPROTO of outbound packets to determine how to set the IPPROTO of the filter spec. The reason for this is that the RSVP PATH and RESV messages must be exchanged before data begins to flow if that data is to be protected. This requirement leads us to develop an RSVP object type to carry the data's 'native' IP protocol field in case a downstream gateway needs to set the IP protocol field of departing SESSION objects to reflect that of the actual, unencrypted, data.

The SESSION_ASSOC object described in RFC 2746 (reference [9]) contains enough information to restore the original IP protocol number (since it contains a copy of the end-to-end SESSION object). However, using a SESSION_ASSOC object to convey the original IP protocol number would be problematic. A better solution is to define a new RSVP object type to carry the original IP protocol number from the upstream to the downstream security gateway.

The proposed new object type would be attached to PATH messages by the RSVP daemon at the upstream NGSI security gateway, and stripped at the downstream security gateway.

3.4.2 RSVP ORIG_IPPROTO OBJECT

NOTE – This subsection defines a new RSVP object type for carrying an IPPROTO number so that it is available to downstream RSVP-capable routers that need it. See figure 3-2, which depicts the format of the ORIG_IPPROTO object.

0	1	2	3
Length (>= 8)		C-Num (in the 224-255 range)	C-Type
ORIG_IPPROTO	Reserved (set to 0 and ignored on receipt)		

Figure 3-2: ORIG_IPPROTO Object

NOTES

- 1 Length: This field contains the size of the ORIG_IPPROTO object in bytes. Thus the length field will contain the decimal value 8.
- 2 Class: A class number from the 224-255 range. Objects of this class are silently ignored but forwarded by RSVP daemons that do not understand them. We are currently seeking class number assignment; future versions of this Experimental Specification will contain the assigned class number.
- 3 Ctype: Ctype should be sent as zero and ignored on receipt.
- 4 ORIG_IPPROTO: The IP Protocol number of the data traffic type, regardless of whether or not encryption will be used (e.g., 6 TCP or decimal 17 for UDP).

3.4.2.1 Generation of ORIG_IPPROTO Objects

ORIG_IPPROTO objects are appended to PATH messages at by data sources if:

- 1) The RSVP PATH messages sent by the source will not contain the ‘native’ IP protocol # of the data (as is the case if the data will be protected with IPSEC, e.g.)
- 2) The source believes that at some point the PATH message will need to reflect the ‘native’ IP protocol # of the data.

These conditions are satisfied in the NGSI architecture depicted in figure 2-1 when the ‘downstream’ NGSI security gateways is configured to forego encryption for outbound data. In this case, the source sets the IP protocol field of generated PATH messages to be IPSEC, and the only way for the downstream security gateway to send reasonable PATH messages with the data’s native IP protocol number is to use the ORIG_IPPROTO object.

Note that if the downstream security gateway implements security on both sides (e.g., SCPS-SP on one side and IPSEC on the other), then the RSVP daemon knows the outbound IP protocol number (50, IPSEC ESP in this case). For these cases, data sources do not need to include ORIG_IPPROTO objects with their PATH messages.

3.4.2.2 Processing of ORIG_IPPROTO Objects

The RSVP daemons in NGSI security gateways need to check for the presence of ORIG_IPPROTO objects when forwarding PATH messages when the outbound IP protocol

number of the corresponding data packets is not known *a priori*. The value of the ORIG_IPPROTO field can then be used in outbound SESSION objects to correctly reserve resources for the flow.

4 CONCLUSIONS

The NGSI project has defined an architecture and technologies that will allow future sensor webs connected to the Internet to manage data flows and node mobility, and to provide security in a dynamic, networked environment. The data flow management aspect of NGSI is accomplished through adoption of the Internet's Resource Reservation Protocol (RSVP). This Experimental Specification describes how RSVP can be used to manage data flows within the NGSI architecture, and defines a new RSVP object type necessary to allow RSVP to function correctly in concert with the NGSI security gateways. It has also examined some of the deployment issues related to RSVP use in the Internet.

ANNEX A

ABBREVIATIONS AND ACRONYMS

AIST	Advanced Information Systems Technology
CCSDS	Consultative Committee for Space Data Systems
GPI	Generic Port Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
NGSI	Next Generation Space Internet
PI	Principal Investigator
QoS	Quality of Service
RFC	Request for Comments
RSVP	Resource Reservation Protocol
SCPS	Space Communications Protocol Specification
SCPS-SP	Space Communications Protocol Specification-Security Protocol
UDP	Universal Datagram Protocol
VPN	Virtual Private Network

ANNEX B

INFORMATIVE REFERENCES

- [1] Y. Bernet, P. Ford, R. Yavatkar, F. Baker, L. Zhang, M. Speer, R. Braden, B. Davie, J. Wroclawski, E. Felstaine. *A Framework for Integrated Services Operation over Diffserv Networks*. RFC 2298, November 2000.
- [2] Nichols, K., Blake, S., Baker, F. and D. Black. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, December 1998.
- [3] Black, D., Blake, S., Carlson, M., Davies, E., Wang, Z. and W. Weiss. *An Architecture for Differentiated Services*. RFC 2475, December 1998.
- [4] Baker et. al. *RSVP Cryptographic Authentication*. RFC 2747, January 2000.
- [5] JUNOS 4.3 Internet Software Configuration Guide: MPLS Applications.
- [6] Bernet, Y. *Format of the RSVP DCLASS Object*. RFC 2996, November 2000.