Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 21, 2008

J. Manner
TKK
R. Bless
Univ. of Karlsruhe
January 18, 2008

What is Next Steps in Signaling anyway - A User's Guide to the NSIS Protocol Family
draft-manner-nsis-user-guide-00.txt

Status of this Memo

Copyright Notice

Abstract

The Next Steps in Signaling (NSIS) Working group was officially formed in November 2001 to standardize a new IP signaling protocol suite. Six years have now passed and the first actual protocol specifications have been finalized. The purpose of this draft is to give an overview of what has been achieved, how the industry can make use of the new protocols, and how the research community can further

extend the designs.

Table of Contents

1. Introduction

The Transport Area Directors held a Next Steps in Signaling (NSIS) birds of a feather session on Wednesday 21st March 2001 at the 50th IETF meeting in Minneapolis. The goal of the session was to discuss and gather an initial set of requirements for a next generation Internet signaling protocol suite as it was felt that the current RSVP-based solutions have short-comings, e.g., with respect to mobility or QoS interoperability. The NSIS Working Group was officially formed later that year, in November 2001 and had its first meeting at the IETF 52 in Salt Lake City in December 2001.

The initial charter of NSIS was focused on QoS signaling as the first use case, taking RSVP as the background for the work. In May 2003, middlebox traversal was added as an explicit second use case. The requirements for the new generation of signaling protocols are documented in [RFC3726] and an analysis of existing signaling protocols can be found in [RFC4094].

The design of NSIS is based on a two-layer model, where a general signaling transport layer provides services to an upper signaling layer. The design was influenced by Bob Braden's Internet Draft entitled "A Two-Level Architecture for Internet Signaling" [I-D.braden-2level-signal-arch].

This document gives an overview of what the NSIS framework is today, provides help and guidelines to the reader as to how NSIS can be used in an IP network, and how the protocol can be enhanced to fulfill new use cases.

2. The NSIS Architecture

The design of the NSIS protocol suite reuses ideas and concepts from RSVP but essentially divides the functionality into two layers. The lower layer, the NSIS Transport Layer Protocol (NTLP), is in charge

of transporting the higher layer protocol messages to the next signaling node on the path. This includes discovery of the next hop NSIS node, which may not be the next routing hop, and different transport services depending on the signaling application requirements. The General Internet Signaling Transport (GIST) is the protocol that fulfills the role of the NTLP. The NSIS suite supports both IP protocol versions, IPv4 and IPv6.

The actual signaling application logic is implemented in the higher layer of the NSIS stack, the NSIS Signaling Layer Protocol (NSLP). While GIST is only concerned in transporting NSLP messages between two end-points, the end-to-end signaling functionality is provided by

the NSLP protocols if needed - not all NSLP protocols need to perform end-to-end signaling, even the current protocols have features to confine the signaling to a limited path. Two NSLP protocols are currently standardized: one concerning Quality of Service signaling and one for NAT/Firewall traversal.

A central concept of NSIS is the Session Identifier (SID). Signaling application states are indexed and referred to through the SID. This decouples the state information from IP addresses, allowing dynamic IP address changes for signaling flows, e.g. due to mobility: changes in IP addresses do not force complete tear down and re-initiation of a signaling application state, merely an update of the state parameters.

The SID is not meaningfull by itself, but is rather used together with the NSLP identifier (NSLPID) and the Message Routing Information (MRI). This 3-tuple is used by GIST to index and manage the signaling flows.

The following design restrictions were imposed for the first phase of the protocol suite. They may be lifted in future and new functionality may be added into the protocols at some later stage.

- Path-coupled signaling only: GIST transports messages towards an identified unicast data flow destination based on the signaling application request, and does not directly support path-decoupled signaling, e.g., QoS signaling to a bandwidth broker. The framework also supports a "Loose-End" message routing method used to discover GIST nodes with particular properties in the direction

of a given address, for example the NAT/FW NSLP uses this method to discover a NAT along the upstream data path.

- No multicast support: Introducing support for multicast was deemed too much overhead, if considering the currently limited support for global IP multicast. Thus, the current GIST and the NSLP specifications consider unicast flows only.

The key documents specifying the NSIS protocol suite are:

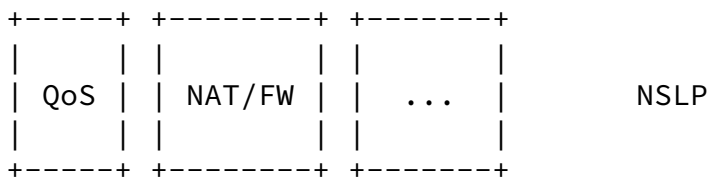
- Requirements for Signaling Protocols [RFC3726]
- Next Steps in Signaling: Framework [RFC4080]
- Security Threats for NSIS [RFC4081]
- The General Internet Signaling Transport protocol [I-D.ietf-nsis-ntlp]
- Quality of Service NSLP [I-D.ietf-nsis-qos-nslp]
- The QoS specification template [I-D.ietf-nsis-qspec]
- NAT/Firewall traversal NSLP [I-D.ietf-nsis-nslp-natfw]

The next three sections provide a brief survey of GIST, QoS NSLP, and

NAT/FW NSLP.

3. The General Internet Signaling Transport

The General Internet Signaling Transport (GIST) [I-D.ietf-nsis-ntlp] provides a signaling transport service to NSIS Signaling Layer Protocols (NSLP). GIST does not define new IP transport protocols but rather makes use of existing protocols, such TCP and UDP. Applications can indicate the desired reliability, e.g., unreliable or reliable, and GIST then uses the most appropriate transport protocol to achieve the goal. If applications request also security, GIST uses TLS. The GIST layered protocol stack is shown in Figure 1.



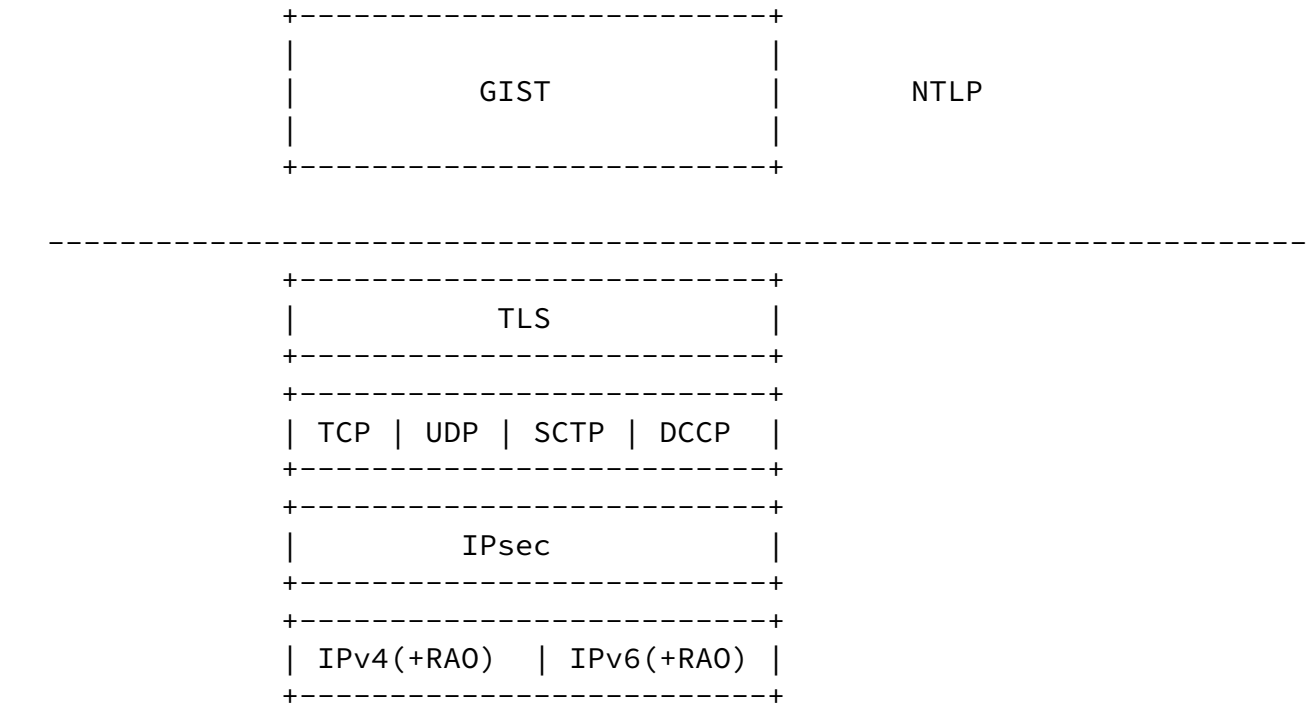


Figure 1: The NSIS protocol stack

When an NSLP application wants to send a message to its next peer, GIST starts discovering the next signaling node by sending a Query

message towards the destination of the related data flow. This Query carries the NSLP identifier (NSLP ID) and Message Routing Information (MRI) among others. The MRI contains enough information to route the signaling message, e.g., information about the actual data flow that is signaled for. The next GIST node on the path receives the message and if it is running the same NSLP, it provides the MRI to the NSLP application and requests it to make a decision on whether to peer with the querying node. If the NSLP application chooses to peer, GIST sets up a Message Routing State (MRS) between the two nodes for the future exchange of NSLP data. State setup is performed by a three-way handshake that allows for negotiation of signaling flow parameters and provides counter-measures against several attacks like denial-of-service by using cookie mechanisms and a late state installation option.

If a transport connection is required and set up for reliable or secure signaling, like TCP or TLS/TCP, a Messaging Association (MA) is established between the two peers. An MA can be re-used for signaling messages concerning several different data flows, i.e., signaling messages between two nodes are multiplexed over the same transport connection. This can be done when the transport requirements (reliability, security) of a new flow can be met with an existing MA, i.e., the security and transport properties of an existing MA are equivalent or better than what is requested by the new MA.

For path-coupled signaling, we need to find the nodes on the data path that should take part in the signaling of an NSLP and invoke them to act due to arrival of such NSLP signaling messages. The basic concept is that such nodes along a flow's data path intercept the corresponding signaling packets and are thus discovered automatically. GIST uses by default the Router Alert Option (RAO) in Query messages to tell a receiving router that the packet must be inspected and possibly taken out of the fast path. This is the the same mechanism as in RSVP. Different RAO values can be used to indicate the actual NSLP being signaled, thus, making it possible for routers to leave the packet in the fast path if the right NSLP protocol is not available on the router; only a router that runs GIST and the corresponding NSLP will take the packet out of the fast path, and start processing it within GIST. Further intentional bypassing of signaling nodes can be accomplished either in GIST or in the NSLP.

Since GIST carries information about the data flow inside its messages (in the MRI), NAT gateways must be aware of GIST in order to let it work correctly. GIST provides a special object for NAT traversal so that the actual translation is disclosed if a GIST-aware NAT gateway provides this object.

GIST may use different triggers in order to detect a route change. It probes periodically for the next peer by sending a GIST Query, thereby detecting a changed route and GIST peer. GIST monitors routing tables, the GIST peer states, and notifies NSLPs of any routing changes. It is up to the NSLPs to act appropriately then, if needed, e.g., by issuing a refresh message.

In summary, GIST provides several services in one package to the

upper layer signaling protocols:

- Signaling peer discovery: GIST is able to find the next hop node that runs the NSLP being signaled for.
- Multiplexing: GIST reuses already established signaling relationships and messaging associations to peers if the signaling flows traverse the same next signaling hop.
- Transport: GIST provides transport with different attributes, namely reliable/unreliable and secure/unsecure.
- Confidentiality: If security is requested, GIST uses TLS to provide an encrypted and integrity protected message transport to the next signaling peer.
- Routing changes: GIST detects routing changes, but instead of acting on its own, it merely sends a notification to the local NSLP. It is then up to the NSLP to act.
- Fragmentation: GIST uses either a known Path MTU for the next hop or limits its message size to 576 bytes. If fragmentation is required it automatically establishes an MA and sends the signaling traffic over a reliable protocol, e.g., TCP.

4. Quality of Service NSLP

The Quality of Service (QoS) NSIS Signaling Layer Protocol (NSLP) establishes and maintains state at nodes along the path of a data flow for the purpose of providing some forwarding resources for that flow. It is intended to satisfy the QoS-related requirements of RFC 3726 [RFC3726]. No support for QoS architectures based on bandwidth brokers is currently included.

The design of the QoS NSLP is conceptually similar to RSVP, RFC 2205 [RFC2205], and uses soft-state peer-to-peer refresh messages as the primary state management mechanism (i.e., state installation/refresh is performed between pairs of adjacent NSLP nodes, rather than in an end-to-end fashion along the complete signaling path). The QoS NSLP extends the set of reservation mechanisms to meet the requirements of RFC 3726 [RFC3726], in particular support of sender or receiver-initiated reservations, as well as, a type of bi-directional reservation and support of reservations between arbitrary nodes, e.g., edge-to-edge, end-to-access, etc. On the other hand, there is

currently no support for IP multicast.

A distinction is made between the operation of the signaling protocol and the information required for the operation of the Resource Management Function (RMF). RMF-related information is carried in the QSPEC (QoS Specification) [I-D.ietf-nsis-qspec] object in QoS NSLP messages. This is similar to the decoupling between RSVP and the IntServ architecture, RFC 1633 [RFC1633]. The QSPEC carries information on resources available, resources required, traffic descriptions and other information required by the RMF.

QoS NSLP supports different QoS models, because it does not define the QoS mechanisms and RMF that have to be used in a domain. As long as a domain knows how to perform admission control for a given QSPEC, QoS NSLP actually does not care how the specified constraints are enforced and met, e.g., by putting the related data flow in the topmost of four DiffServ classes, or by putting it into the third highest of twelve DiffServ classes. The particular used QoS configuration is up to the network provider of the domain. The QSPEC can be seen as a common language to express QoS requirements between different domains and QoS models.

In short, the functionality of the QoS NSLP includes:

- Conveying resource requests for unicast flows
- Resource requests (QSPEC) are decoupled from the signaling protocol (QoS NSLP)
- Sender- and receiver-initiated reservations, as well as, bi-directional
- Soft state and reduced refresh (keep-alive) signaling
- Session binding, session X can be valid only if session Y is too
- Message scoping, end-to-end, edge-to-edge or end-to-edge (proxy mode)
- Protection against message re-ordering and duplication
- Group tear, tearing down several session with a single message
- Support for re-routing, e.g., due to mobility
- Support for request priorities and pre-emption
- Stateful and stateless nodes
- Reservation aggregation

5. NAT/Firewall Traversal NSLP

The NAT/Firewall Traversal NSLP [I-D.ietf-nsis-nslp-natfw] lets end-hosts interact with NAT and firewall devices in the data path. Basically it allows for a dynamic configuration of NATs and/or firewalls along the data path in order to enable data flows to traverse these devices without being obstructed. For instance, firewall pinholes could be opened on demand by authorized hosts.

Furthermore, it is possible to block unwanted incoming traffic on demand, e.g., if an end-host is under attack.

Basically NATFW signaling starts at the data sender (NSIS Initiator) before any actual application data packets are sent. Signaling messages may pass several NATFW NSLP-aware middleboxes (NSIS Forwarder) on their way downstream and usually hit the receiver (being the NSIS Responder). A proxy mode is also available for cases where NATFW is not fully supported along the complete data path. NATFW NSLP is based on a soft-state concept, i.e., the sender must periodically repeat its request in order to keep it active.

Additionally, the protocol also provides functions for receivers behind NATs. The receiver may request an external address that is reachable from outside. The reserved external address must, however, be communicated to the sender out-of-band by other means, e.g., by application level signaling. After this step the data sender may initiate a normal NATFW signaling in order to create firewall pinholes.

6. Deploying the Protocols

First of all, NSIS implementations must be available in the corresponding network nodes (i.e., routers, firewalls, or NAT gateways) and end-hosts. That means not only GIST support, but also the NSLPs and their respective control functions (such as a resource management function for QoS admission control etc.) must be implemented. In dependence on the specific NSLP, scenarios are also supported where only one end-host is NSIS-capable and the end-host on the other is not NSIS-capable. This is usually accomplished by performing some kind of proxying functions in the domain of the responding end-host.

Another important issue is that applications must be made NSIS-aware, thereby requiring some effort on the applications programmer's side. Yet, it is possible to implement separate applications to control, e.g., the network QoS requests or firewall holes.

6.1. Obstacles

As there is network equipment with broken implementations of the Router Alert Option deployed, there may be some obstacles for initial deployment due to this legacy equipment. For controlled environments an operation without RAO is also possible as GIST uses a specific UDP port and a special magic number in order to detect Query signaling

messages reliably.

NAT gateways and firewalls may also hinder initial deployment of NSIS protocols as they may either filter signaling traffic or perform NSIS-unaware address translations.

7. Security Features

Basic security functions are provided at the GIST layer, e.g., protection against some blind or denial-of-service attacks. Conceptually it is difficult to protect against on-path attacker and man-in-the-middle attacks, because a basic functionality of GIST is to discover yet unknown signaling peers. Transport security can be requested by signaling applications and is realized by using TLS between signaling peers, i.e., authenticity and confidentiality of signaling messages can be assured between peers. GIST allows for mutual authentication of the signaling peers (using TLS means like certificates) and can verify the authenticated identity against a database of nodes authorized to take part in GIST signaling. It is, however, a matter of policy that the identity of peers is verified and accepted upon establishment of the secure TLS connection.

While GIST is handling authentication of peer nodes, more fine grained authentication may be required in the NSLP protocols. There is currently an ongoing work to specify common authorization mechanisms to be used in NSLP protocols [I-D.manner-nsis-nslp-auth], thus allowing, e.g., per-user and per-service authorization.

8. Extending the Protocols

This section discusses the ways to extend the NSIS protocols. One key functionality of all three current protocols are the so-called "Extensibility flags (AB)". The protocols can carry new experimental objects, where the AB-flags can indicate whether a receiving node must interpret the object, or whether it can just drop them or pass them along in subsequent messages sent out further on the path. This functionality allows defining new objects without forcing all network entities to understand them.

8.1. GIST

GIST is extensible in several aspects.

- Use of different Message Routing Methods. Currently only two message routing methods are supported (Path-coupled MRM and Loose-End MRM), but further MRMs may be defined in the future.
- Use of different transport protocols. The initial handshake allows a negotiation of the transport protocols to be used. Currently, a proposal to add DCCP and DTLS to GIST exists [I-D.manner-nsis-gist-dccp].
- The AB-flags enable the community to specify new objects into GIST, that can be carried inside a signaling session without breaking existing implementations. The AB-flags can also be used to indicate in a controlled fashion that a certain object must be understood by all GIST nodes, which makes it possible to probe for the support of an extension. One such object already designed is the "Peering Information Object (PIO)" [I-D.manner-nsis-peering-data] that allows a QUERY message to carry additional peering data for the recipient for making the peering decision.

8.2. QoS NSLP

A foreseen development within the QoS signaling is the introduction of new QoS Models to enable deployment of NSIS in specific scenarios. One such example is the Integrated Services Controlled Load Service for NSIS [I-D.kappler-nsis-qosmodel-controlledload].

There is already work to extend the base QoS NSLP and GIST to enable new QoS signaling scenarios. One such proposal is the Inter-Domain Reservation Aggregation aiming to support large-scale deployment of the QoS NSLP [I-D.bless-nsis-resv-aggr]. Another current proposal seeks to extend the whole NSIS framework towards path-decoupled signaling and QoS reservations [I-D.cordeiro-nsis-hypath].

8.3. NAT/Firewall NSLP

The NATFW signaling can be extended in the same way as the QoS NSLP. No proposals currently exist to fulfill new use cases for the protocol.

8.4. New NSLP protocols

Designing a new NSLP is both challenging and easy. On one hand, GIST provides many important functions through its service layer API, and allows the signaling application programmer to offload, e.g., the channel security, transport characteristics and signaling node discovery to GIST.

Yet, on the other hand, the signaling application designer must take into account that the network environment can be dynamic, both in terms of routing and node availability. The new NSLP designer must take into account at least the following issues:

- Routing changes, e.g., due to mobility: GIST sends Network Notifications when something happens in the network, e.g., peers or routing paths change. All signaling applications must be able to handle these notifications and act appropriately. GIST does not include logic to figure out what the NSLP would want to do due to a certain network event. Therefore, GIST gives the notification to the application, and lets it make the right decision.
- GIST indications: GIST will also send other notifications, e.g., if a signaling peer does not reply to refresh messages, or a certain NSLP message was not successfully delivered to the recipient. Again, NSLP applications must be able to handle these events, too. Appendix B in the GIST specification discusses the GIST-NSLP API and the various functionality required, but implementing this interface can be quite challenging; the multitude of asynchronous notifications than can from GIST increases the implementation complexity of the NSLP.
- Lifetime of the signaling flow: NSLPs should inform GIST when a flow is no longer needed using the SetStateLifetime primitive. This reduces bandwidth demands in the network.
- NSLP IDs: there is a limited number of NSLP IDs available for experimental use. In practise, a new signaling protocol will eventually require its own NSLP ID number.
- Source IP address: It is sometimes challenging to find out at the NSLP, what will the source IP address be, especially when a node has multiple interfaces. Moreover, the logic in specifying the source IP address may differ if the node processing an NSLP message is the source of the signaling flow, or an intermediate

node on the signaling. Thus, the NSLP must be able to find out the right source IP address from its internal interfaces, and its location on the signaling.

- New MRMs: GIST defines currently two Message Routing Methods, and leave the door open for new ideas. Thus, it is possible that a new NSLP also requires a new MRM, path-decoupled routing being one example.

The informational API between GIST and NSLPs (see Appendix B in [I-D.ietf-nsis-ntlp]) is very important to understand. It does not specify the exact messaging between GIST and the NSLPs but gives an understanding of the interactions, especially what kinds of asynchronous notifications from GIST the NSLP must be prepared to handle.

9. Security Considerations

This document provides information to the community. It does not raise new security concerns.

10. Acknowledgements

Max Laier, Nuutti Varis and Lauri Liuhto have provided reviews of this draft and valuable input.

11. References

11.1. Normative References

[I-D.ietf-nsis-nslp-natfw]
Stiemerling, M., Tschofenig, H., Aoun, C., and E. Davies, "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-16 (work in progress), November 2007.

[I-D.ietf-nsis-ntlp]
Schulzrinne, H. and R. Hancock, "GIST: General Internet

Signalling Transport", draft-ietf-nsis-ntlp-14 (work in progress), July 2007.

[I-D.ietf-nsis-qos-nslp]
Manner, J., "NSLP for Quality-of-Service Signaling", draft-ietf-nsis-qos-nslp-15 (work in progress), July 2007.

[I-D.ietf-nsis-qspec]
Ash, G., Bader, A., Kappler, C., and D. Oran, "QoS NSLP QSPEC Template", draft-ietf-nsis-qspec-18 (work in progress), October 2007.

[RFC3726] Brunner, M., "Requirements for Signaling Protocols", RFC 3726, April 2004.

[RFC4080] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[RFC4081] Tschofenig, H. and D. Kroeselberg, "Security Threats for Next Steps in Signaling (NSIS)", RFC 4081, June 2005.

11.2. Informative References

[I-D.bless-nsis-resv-aggr]
Doll, M. and R. Bless, "Inter-Domain Reservation Aggregation for QoS NSLP", draft-bless-nsis-resv-aggr-01 (work in progress), July 2007.

[I-D.braden-2level-signal-arch]

Braden, R. and B. Lindell, "A Two-Level Architecture for Internet Signaling", draft-braden-2level-signal-arch-01 (work in progress), November 2002.

[I-D.cordeiro-nsis-hypath]
Cordeiro, L., "GIST Extension for Hybrid On-path Off-path Signaling (HyPath)", draft-cordeiro-nsis-hypath-04 (work in progress), July 2007.

[I-D.kappler-nsis-qosmodel-controlledload]
Kappler, C., "A QoS Model for Signaling IntServ

Controlled-Load Service with NSIS",
draft-kappler-nsis-qosmodel-controlledload-05 (work in
progress), July 2007.

[I-D.manner-nsis-gist-dccp]
Manner, J., "Generic Internet Signaling Transport over
DCCP and DTLS", draft-manner-nsis-gist-dccp-00 (work in
progress), June 2007.

[I-D.manner-nsis-nslp-auth]
Manner, J., "Authorization for NSIS Signaling Layer
Protocols", draft-manner-nsis-nslp-auth-03 (work in
progress), March 2007.

[I-D.manner-nsis-peering-data]
Manner, J., "Peering Data for NSIS Signaling Layer
Protocols", draft-manner-nsis-peering-data-00 (work in
progress), June 2007.

[RFC1633] Braden, B., Clark, D., and S. Shenker, "Integrated
Services in the Internet Architecture: an Overview",
RFC 1633, June 1994.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S.
Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1
Functional Specification", RFC 2205, September 1997.

[RFC4094] Manner, J. and X. Fu, "Analysis of Existing Quality-of-
Service Signaling Protocols", RFC 4094, May 2005.

Authors' Addresses

Jukka Manner
Helsinki University of Technology (TKK)

P.O. Box 3000
Espoo FIN-02015 TKK
Finland

Phone: +358 9 451 2481
Email: jukka.manner@tkk.fi
URI: http://www.netlab.tkk.fi/~jmanner/

Roland Bless
Institute of Telematics, Universitaet Karlsruhe (TH)
Zirkel 2
Karlsruhe 76128
Germany

Phone: +49 721 608 6413
Email: bless@tm.uka.de
URI: http://www.tm.uka.de/~bless

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).