A Problem Statement for Path-Decoupled Signalling in NSIS
draft-hancock-nsis-pds-problem-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on November 18, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The NSIS working group is currently developing a protocol suite for signalling which manipulates network state related to data flows. The protocol architecture incorporates the constraint that the signalling protocol will be processed on the nodes which also handle...
the data flows themselves ("path-coupled signalling"). This document
discusses motivations for a relaxation of this constraint, allowing
the signalling and data paths to be decoupled. It includes several
scenarios and pointers to related work elsewhere in the IETF and in
other standardisation bodies, and includes a recommendation that the
NSIS work should be extended to cover these types of architectures.

Table of Contents

1. Introduction ........................................... 3
2. Motivation ............................................. 4
   2.1 Centralised Policy Control ....................... 4
   2.2 Intradomain Centralised Monitoring and Resource
        Management ........................................ 4
   2.3 Interdomain Off-Path Signalling .................. 6
   2.4 3rd Party Signalling Initiation .................. 6
   2.5 Signalling on multiple (candidate) paths ........ 7
   2.6 Architectures of Other SDOs ..................... 8
3. Network Configurations ................................ 8
   3.1 Baseline NSIS Operation ......................... 9
   3.2 NSIS with Policy Outsourcing .................... 9
   3.3 Off-Path Intradomain NSIS ....................... 10
   3.4 Interdomain Off-Path Signalling ................. 11
   3.5 Signalling on Multiple Candidate Paths ......... 12
   3.6 Off-path NSIS Initiator and Responder .......... 12
4. Problem Structure ..................................... 13
   4.1 Signalling Backhaul .............................. 14
   4.2 Network Element Control .......................... 15
   4.3 Router Determination .............................. 15
   4.4 Off-Path Transport ................................ 15
   4.5 Signalling Node Identification ................. 16
   4.6 Host Proxy Triggering ......................... 17
   4.7 Multi-Path Selection ............................. 17
5. Security Considerations .............................. 18
6. Conclusions .......................................... 19
7. References .......................................... 19
   7.1 Normative References ............................ 19
   7.2 Informative References .......................... 19
   Authors’ Addresses .................................. 21
A. Acknowledgements .................................. 22
   Intellectual Property and Copyright Statements .... 23
1. Introduction

The NSIS working group is currently developing a protocol suite for signalling which manipulates network state related to data flows. Requirements for such signalling are contained in [1][2][3] and a framework which describes a layered protocol architecture is given in [4]. The architecture consists of a lower layer which is common to all signalling applications, the NSIS Transport Layer Protocol (NTLP), and separate upper layer protocols which implement the application specific logic, called NSIS Signalling Layer Protocols (NSLPs). The current design of the NTLP is known as GIMPS [5], and NSLPs for QoS signalling and middlebox control are given in [6] and [7] respectively.

The current NSIS work concentrates on the so-called ‘path-coupled’ case (see section 3.1.2 of [4]), where the signalling messages pass through a sequence of nodes which is a subset of the nodes (end hosts and routers) on the path taken by the data flow being signalled for. However, it has become clear that there is considerable interest in a more flexible set of network configurations, where the signalling still refers to current or future data flows but is less tightly constrained to follow the flow path. The ability to arrange components of the signalling solution in this way gives some additional engineering flexibility which can be very valuable in certain operational environments; this has been recognised in other IETF activities such as PCE [8], IPFIX [9], and PSAMP [10], and also in the signalling architectures assumed by other standardisation bodies (see Section 2.6). Even when these other configurations are considered, it is clear that there are still large elements of the overall signalling solution that remain common, specifically the semantics of signalling application transactions and the language in which state manipulation is specified. Therefore, we believe that it is important to investigate whether the NSIS protocols can be extended to cover these scenarios. This would have the additional advantage that signalling solutions would not fragment into ‘on-path’ and ‘off-path’ worlds - and that indeed, mixed configurations could be commonplace, served by a single overall protocol suite.

It is the purpose of this draft to give an overview of the engineering motivations for path-decoupled signalling concepts, and to begin to explore how they could be accommodated within the current NSIS framework. The remainder of this document is structured as follows. Section 2 describes some very high level usage scenarios, explaining the motivations for the basic concepts of path-decoupled signalling, and Section 3 places these scenarios in a set of concrete network configurations, showing the entities involved and listing the components needing to make a complete solution. Section 4 describes these components in more detail. Security considerations are given...
2. Motivation

This section introduces various high-level scenarios to motivate the use of off-path signalling for data flows, describing some of the engineering advantages that can be achieved. The description is high-level and not related to specific NSIS concepts or concrete network configurations (these topics are introduced in Section 3, which also discusses what additional functionality would be needed to support such solutions). However, it does include references to the signalling architectures of other Standards Development Organisations (SDOs) which use such approaches.

2.1 Centralised Policy Control

It is commonplace to want to be able to carry out some of the policy-related processing needed for a signalling transaction on a node separate from the routers themselves. There are several reasons for this:

- The policy processing may be computationally demanding and very variable in load. It therefore makes sense to decouple the platform for this from the platform handling the user plane itself so they can be scaled separately.

- The policy processing requirements may evolve independently from (and probably more rapidly than) the basic resource signalling requirements.

- The same policy processing may be needed for several nodes within a single domain. Using a dedicated node for this therefore allows some centralisation of resources, and also concentrates interfaces towards other network functions (such as accounting).

Policy centralisation alone is not the main theme of this document, since there are already a number of solutions available or under consideration. However, most of the other path-decoupled scenarios include similar characteristics and have the same motivations, and it would be sensible for implementation approaches to re-use parts of these solutions where possible.

2.2 Intradomain Centralised Monitoring and Resource Management

In many scenarios, as well as servers for outsourced policy control, there are central nodes which maintain an overview of the resource utilisation status of the network (this is particularly the
assumption in PCE work [19], for example). Such nodes are commonplace in operator networks because they allow monitoring the network status in order to take corrective action quickly if needed. Under these circumstances, there are advantages if the signalling protocol can be executed directly at the same nodes. More concretely, we can model the overall resource management problem as four components (compare e.g. figure 1 of the QoS-NSLP specification [6]):

1. Operation of the signalling protocol state machine

2. Decision making about resource availability and allocation (admission/policy control)

3. Finally, resource configuration in the user plane (which by definition must take place on-path)

4. Some kind of transaction management to bind items (1-3) together in the correct sequence

In the baseline NSIS model, all four components are colocated on-path. Policy outsourcing moves some part of (2) off-path, but the transaction control remains on-path and must bind together the operation of the signalling and policy protocols, as well as the actual resource configuration steps. The assumption of the centralised resource management scenario is that all of (1) and (2) and the synchronisation between them can be moved off-path to nodes which manage a whole set of routers.

This model less precise synchronisation of transaction management between the on/off path nodes than in the policy outsourcing case. If the resource availability information is already being gathered centrally for other reasons, the only additional interaction is the resource configuration which can be done in parallel for all on the on-path nodes, rather than having to be done along the sequence of on-path nodes. It can also usually be done asynchronously with the signalling transactions (unless for example pre-emption is required). Even if specific resource availability information has to be gathered, again this can be done in parallel for all the on-path nodes. These two advantages - parallelisation of the per-on-path node operation and decoupling between signalling/control transactions and resource configuration - allow centralised resource management to achieve better overall control-plane performance than the policy outsourcing approaches, but with the same benefits from the independence between control and user plane implementations.

This scenario is also a highly attractive intermediate step when migrating an administrative domain towards full NSIS support.
Typically, not all routers in a domain can be updated to NSIS or replaced with NSIS-capable equipment at the same time. The scenario allows support of NSIS towards the outside with only the edge routers and the central controllers implementing this new protocol. The internal support by all routers can be achieved at a later point in time. Then the central control function concerning NSIS would become obsolete.

2.3 Interdomain Off-Path Signalling

In principle, centralised resource management approaches can be deployed internally as a matter of network operator choice, while still using ‘classic’ NSIS on-path signalling on external links. However, where neighbouring domains are both using such centralised approaches, there may be benefits if they are able to signal directly to each other rather than stepping back to on-path signalling for the single inter-domain hop. The main point is that such interdomain signalling is likely to be associated with other interdomain operations such as AAA; therefore, it is attractive if the signalling associations involved are long-lived and small in number (since they will be expensive to create and manage). In particular, a route change at the node level which does not affect the path at the interdomain level should not require the creation and correlation of two interdomain signalling transactions. Another issue is that operators may wish to segregate such control traffic from user traffic physically for security reasons (e.g. continued operation under overload) and this is much harder in the pure on-path case.

2.4 3rd Party Signalling Initiation

In this scenario, the signalling is not directly initiated by the flow endpoint but rather by an off-path node having enough knowledge to initiate the signalling. Examples for this include where an end node cannot be trusted to start and control the signalling, where a 3rd party off-path node is interested in on-path information, or where the flow end node does not have the necessary information or ability to operate the complete signalling exchange. This scenario also covers the case of a domain recently migrated to NSIS, but supporting legacy non-NSIS aware devices.

An example of operation is that the flow endpoint requests an application-specific service by sending a "Service Request" (for example a SIP message) to a service controller. It is then the service controller’s responsibility to determine the resource needs of the requested service, and to communicate these needs to a proxy which then initiates signalling on behalf of the flow endpoint. Such scenarios are described by 3GPP [11] and ETSI [12]. In fact, the QoS management in current xDSL networks is in conformance with this
scenario. A typical scenario for a NAT/Firewall environment is the use of this proxy initiated signalling in large enterprise networks running already SIP-based telephony. It is expected that the installed SIP phones would be upgraded only gradually to support NSIS signalling.

Another example is metering configuration [13]. Usually, the flow endpoint doesn’t have the knowledge or the authorization to configure meters to measure the flow. However, the knowledgeable node, the proxy, is not necessarily located on the data path. The proxy can initiate the signaling by sending it to the first network-owner controlled metering on the data path, from where the signalling proceeds on-path as normal.

Yet another example is that of RSVP Diagnostic Messages [14]. Here a 3rd party node ("Requester") that is not part of the actual session wishes to diagnose the RSVP state installed along a data path. It therefore issues a RSVP DREQ message towards the Sender, which joins the data path at the node at which diagnosis should start. The DREQ message is forwarded hop-by-hop collecting state information for a specified number of hops. The Sender returns the collected information in a DREP message to the Requester. The DREP message can travel directly, or it can reverse the path taken by the DREQ message based on information in ROUTE object collected in the DREQ packet.

Note the off-path node needs to determine the appropriate NSIS Entity at which to rejoin the data path. In constrained topologies (e.g. tree-like access networks) this is not too difficult. If the initiator is actually on the data path, the NSIS signaling in these scenarios is normal on-path NSIS signaling. However, generally, it may not be located on the data path.

2.5 Signalling on multiple (candidate) paths

The current NSIS protocol suite does not support signalling on multiple (candidate) paths. These paths are sets of routers that are not currently on the data path but that may end up on the data path in the future as a result of a network event, such as a node or link failure, an interdomain route change or a policy change. This scenario is particularly useful for make-before-break reservation on back-up paths that are non-shortest path under the current routing and policy configurations, or to support seamless handover in mobility scenarios (see for example [16]). Make-before-break allows pre-reservation of resources on candidate back-up paths in order to allow for fast failover.
2.6 Architectures of Other SDOs

Other SDOs, particularly those originating from the "telecommunications world" typically assume a centralized controller, e.g. for resource management, in each domain.

For example, the QoS architecture for Next Generation Networks of ETSI [12], features a Service Control Function which is responsible in each domain for controlling service requests initiated by a flow senders. This Service Control Function sends resource requests on behalf of the flow sender to a central resource controller (the Network Resource Control Function) in the same domain. The resource controller subsequently initiates a controller-to-controller QoS signaling exchange through all domains along the data path up to the receiving domain.

3GPP is currently specifying an end-to-end QoS solution [15] for interworking with external non-3GPP IP networks. For the external IP networks a variety of QoS architectures are described, both centralized controller-type architectures and distributed IntServ/DiffServ-type architectures. At this point, however, only QoS procedures for scenarios featuring centrally-managed external networks are specified in detail. One of the problems that need to be solved is the interworking of on-path and off-path QoS signaling in scenarios featuring domains with both centralized and distributed QoS control on the same data path.

3. Network Configurations

This section describes some reference network configurations, to explain how the different components of the overall solution interact when they are no longer constrained to all be colocated on the same device. It highlights the differences from the current NSIS operational model and indicates where additional functions are needed.
3.1 Baseline NSIS Operation

The baseline NSIS configuration is that a (sub-)set of routers on the data path also takes part in the signalling protocol, as shown in Figure 1. This is true both within the domain and between domains.

```
+----------------------------------------------------+
|                    +----------+                    |
|              ******|Controller|******              |
|            *       +----------+       *            |
|          *          *        *          *          |
|        *           *          *           *        |
|      *            *            *            *      |
| +--*---+      +--*---+      +---*--+      +---*--+ |
-----| NSIS |--------------------| NSIS |------| NSIS |-----
| #####|Router|######|Router|######|Router|######|Router|#####
| +------+      +------+      +------+      +------+ |
+----------------------------------------------------+
```

The figure also shows the existence of a separate node issuing configuration commands to the routers, and/or carrying out monitoring of router operation. This can be seen as part of network management, and is conceptually only loosely coupled to the signalling (the signalling transactions and network management transactions are not directly interdependent). It is therefore also considered as a possible part of the baseline scenario.

3.2 NSIS with Policy Outsourcing

"Policy outsourcing" is the use of an external server to take responsibility for certain stages of a signalling transaction. The prime example is where the decision about whether a transaction (e.g. allocation of a resource to a flow) is administratively allowed are not taken on the router directly, but the router calls out to a separate policy server and waits for a response to be returned before continuing. This situation is shown in Figure 2 below. Many variants can be built on this basic concept, with different subsets of the NSIS routers calling out to the policy server; in addition, as a side effect of the policy decision making, the policy server can carry out configuration actions on other routers using network management capabilities as discussed above.
This type of policy outsourcing is not the main theme of this draft, since there are already mechanisms to support it. In particular, COPS has been defined as an outsourcing protocol for RSVP in [17], and a Diameter extension has been proposed to accompany the NSIS QoS-NSLP for policy support to the AAA function in [18]. However, policy outsourcing concepts (and solution components) are relevant to support some of the broader off-path scenarios considered below.

3.3 Off-Path Intradomain NSIS

In this configuration, the signalling itself is allowed to go off-path directly to nodes which handles policy control and resource configuration. The simplest case - of a single node handling a whole domain - is shown in Figure 3. Note that, unlike the policy outsourcing case, there is no separate policy protocol shown. The additional functionality needed compared to standard NSIS signalling is the ability for the NSIS routers to discover the NSIS controller (in this case, on ingress), and for the NSIS controller to discover an on-path node to re-attach the signalling to the data path (in this case, on egress).

There are several variants of this basic concept, for example the use of multiple controllers to handle a particular domain which need to discover and signal directly to each other. However, the interdomain link here uses `standard’ NSIS and so the multi-domain configuration is simply a concatenation of several copies of the above picture.
3.4 Interdomain Off-Path Signalling

This configuration is an extension of the previous case. Formally, the requirements to support this are no different (mutual discovery of the on- and off-path nodes by each other). However, there is an extra requirement that the inter-controller discovery procedure must operate between domains, which imposes extra security and operational constraints.

Figure 3: A Single Off-Path NSIS Node

Figure 4: Interdomain Off-Path Signalling
3.5 Signalling on Multiple Candidate Paths

In this network configuration, there are several candidate paths, and the signalling must be able to follow all of them (and also distinguish between current and candidate paths). The additional requirements here depend quite strongly on how the candidate paths are being created and configured. If they are visible somehow in the user plane (e.g. by using a different tunnel address or codepoint etc.), and can be mimicked by GIMPS Query messages, then no additional functionality is required except for the signalling messages to identify explicitly the status of the path they are signalling about. If the candidate paths are known only in some control plane entities, probably those entities need to be queried to provide the information for explicit routing of the messages.

Administrative Domain

+----------------------------------------------------+
|                                                    |
|               +------+      +------+               |
|    %%%%%%%%%%%| NSIS |%%%%%%| NSIS |%%%%%%%%%%%    |
|    %.---------|Router|------|Router|---------.%    |
|    %|                                        |%    |
|    %|                                        |%    |
|    %|                                        |%    |
| +------+      +------+      +------+      +------+ |
-----| NSIS |------| NSIS |------| NSIS |------| NSIS |-----
#####|Router|######|Router|######|Router|######|Router|#####
+----------------------------------------------------+

######### = data path (current)
%%%%%%%%% = data path (candidate)
--------- = signalling messages

3.6 Off-path NSIS Initiator and Responder

This network configuration is supporting migration and other scenarios and is shown in Figure 6. The main requirement on the signalling is discovery of an on-path node, which is common to the various centralised resource management cases; in addition, extensions to the application layer protocols may be needed to convey additional signalling-related information (this depends on the scenario).

Similar considerations apply to non-NSIS hosts that are addressed by NSIS signalling messages. Here the proxy takes over the role of the NSIS Responder, see Figure 7. The proxy interacts with the service controller in order to notify the application of incoming requests and to respond to the NSIS Initiator depending on input from the
service controller.

Figure 6: Off-Path Signalling Initiator Proxy

Figure 7: Off-Path Signalling Responder Proxy

4. Problem Structure

The previous sections have outlined several possible network
configurations where processing of signalling messages takes place at least partly off the data path. Implementing such configurations requires solutions to several inter-related problems; some of these may be considered as natural extensions to the NSIS problem space, while others may use existing protocols or require additional work in some other forum. This section presents a decomposition of the problem space into several independent parts.

4.1 Signalling Backhaul

Some scenarios maintain the sequence of nodes traversed by the NSIS messages as in the standard (path-coupled) case; however, they allow for some or all of the processing associated with the NSIS messages to be carried out on a remote server. We can model this by saying that NSIS continues to operate in a normal (path-coupled) manner; however, the NSIS implementations themselves are allowed to be distributed between the on-path router and supporting nodes. Distribution in this manner requires two related functions:

Server Node Configuration: The node to which the router will outsource the processing needs to be configured. Typically this would be a network management operation on the router; a minimal approach would be to configure an IP address for remote NSIS processing.

Backhaul Protocol: A protocol is needed to transport the signalling messages (or parts of them) between the router and the server node.

There are many different levels at which the on-router and off-router processing could be split. However, three particularly natural ones can be identified.

IP Level: The IP packets carrying the signalling messages are intercepted by the router and forwarded to the server with some additional encapsulation. This approach may be particularly appropriate for legacy environments, since it minimises the level of NSIS awareness required in the router. Instead it uses only custom forwarding for particular packet types, a capability which is common in many routers in some proprietary form (e.g. for off-board firewall processing, caching and so on). The implied requirement is that the signalling packets must be recognisable by the router without deep packet inspection, and the backhaul transport must carry the information which a local NSIS implementation would have exchanged with the IP layer (mainly, what interface a message arrives/leaves on).
NTLP Level: Here, the NTLP is implemented locally on the router. This approach allows new signalling applications to be deployed without router modification, while still allowing closer integration with the router’s IP layer functionality, for example to allow direct routing protocol interactions. The backhaul transport would carry individual signalling messages (NSLP-Data objects) along with the associated control information as given in the GIMPS API.

NSLP Level: Here, each signalling application is implemented on the router, but elements of the signalling application processing call on a remote server. How this should be done depends very much on the details of the application in question, and efficiency and manageability considerations about how the processing should be split. Solutions for particular cases already exist; for example, the use of AAA protocols to outsource authorisation decisions, or COPS for policy processing in RSVP.

4.2 Network Element Control

Element control is essentially a management operation. Here, a general network management protocol might be used (such as SNMP [20] or a proprietary command line interface); or, for particular applications, a more specialised configuration protocol, such COPS in provisioning mode [21] or the protocols under development in netconf [22] and ForCES [23]. It would appear that such protocols are logically outside the scope of NSIS.

4.3 Router Determination

An element control protocol needs to operate on a target router. In some configurations, the target router can be identified directly (e.g. it is the location from which on-path signalling messages are being forwarded); in others, it can be identified using external information (such as topology data). However, where the purpose of the configuration is to control a sequence of routers between a pair of NSIS capable nodes in arbitrary topologies, this requires route recording which is either inefficient (using traceroute) or not possible (because some specific subset of routers is to be selected) using current techniques. However, a specific NSIS extension could be well tuned for such a role.

4.4 Off-Path Transport

Where the actual hop-by-hop signalling path goes off the data path, a protocol is needed to transfer the signalling messages along that signalling path. This problem can be seen in two parts: the
identification of the signalling nodes to carry out the transfer with 
(the subject of the next subsection, Section 4.5), and the transfer 
mechanism itself.

The requirements on the transfer mechanism are not logically distinct 
from the transfer requirements on the base NTLP. For example, there 
should be the same needs for flow and congestion control and 
reliability of the transfer, and also for message integrity and 
confidentiality. The same questions about how to handle the 
multiplexing of small messages, or multiplexing between several 
sessions or logically independent signalling applications would also 
arise.

4.5 Signalling Node Identification

If signalling messages are to be directed to an off-path node, the 
question naturally arises: which one? A related question is that of 
how to re-attach the signalling path to the data path. In fact, 
three cases can be identified:

Divergence: An on-path node needs to identify its neighbour along the 
signalling path, and that node is off-path. The on-path node 
could be provisioned with a server as in the signalling backhaul 
case; or, the peer could be selected using a modification of the 
RSVP-like query mechanism used in GIMPS. The mode of operation 
could be dependent on the interface that the flow takes (e.g. to 
select off-path operation only for ‘domain-internal’ operation).

Propagation: An off-path node needs to identify its neighbour along 
the signalling path, and that node is off-path. The fundamental 
question here is what criteria are used to define the off-path 
neighbour. Several possibilities can be conceived:

* The peer is defined functionally, that is, on the basis of 
support for a particular signalling application or role. 
Routing of signalling messages would probably have to be 
configured statically by management, since there would be no 
dependence on the flow in question or the underlying network 
topology.

* The peer is defined with respect to the remainder of the flow 
path beyond the set of routers under ‘local’ control. This is 
a combination of the ‘divergence’ case (above) and 
‘convergence’ case (below), since the discovery process depends 
on the local topology and has to take place in the context of 
the current path.
Convergence: An off-path node needs to identify its neighbour along the signalling path, and wishes that node to be on-path (e.g. for compatibility with a peer domain). The discovery process must be path-coupled in some sense, and in particular must take account of the flow path even in the off-path region. Note that there are security aspects to be considered here, since the off-path node could be detected as an off-path attacker in some scenarios, rather than a bona fide signalling peer.

In general, the peer discovery problem appears to be the most complex part of the off-path signalling story, because of the wide variety of discovery mechanisms that can be considered, and also because of the intrinsic hardness of the problem (because of the interactions with network topology and the expectation of needing to maintain compatibility with the pure path-coupled case). However, it also seems that it would have to be considered at least partly within the NSIS problem scope, both because the equivalent problem is clearly an NTLP problem in the path-coupled case, and also because of the compatibility issue just mentioned. Even if some aspects of the configuration of the set of off-path signalling nodes could be considered as network management problems, the topological interactions cannot.

4.6 Host Proxy Triggering

In at least one configuration, the signalling is initiated off-path, typically because the end-host is NSIS-unaware. (This might be the case for either end of a data flow, sending or receiving.) As well as the general problems of transporting the signalling off-path (see Section 4.4) and determining the next peer to signal to (see Section 4.5), this scenario raises an addition special requirement: the need to interact with the user application for whose flows the signalling is being performed.

The implication of this is that the signalling node in question can be assumed to taking part in the user application protocols which are setting up the flows themselves. How the signalling node and flow endpoint determine each other and communicate at this application level can be assumed to be outside the scope of NSIS; a typical case would be where the signalling node was also a proxy for the user application protocol. The signalling specific requirement is that the host and proxy should not initiate colliding signalling sessions.

4.7 Multi-Path Selection

One scenario considers the use of NSIS to signal for state management on alternate paths that a flow would take under certain conditions. (The typical case is for pre-installation of state on backup paths...
that would be selected in network failure situations.) In so far as signalling is not following the current flow, this can be considered a case of path-decoupled signalling.

The requirements for this type of signalling are very similar to the normal path-coupled case, and a very similar split of responsibilities between network, common signalling layer (NTLP), and signalling application is possible. The extra sophistication needed is two-fold:

- The underlying network layer must have the concept of multiple routes of different status (primary, backup, etc.) When the NTLP is establishing the peer node for signalling about a certain flow, the ideal case is that it can do so by using the normal path-coupled discovery process using signalling packets which emulate that flow, but explicitly invoking the routing infrastructure to treat those packets according to its alternate routing algorithms (however those are identified).

- The application which generates the signalling must indicate and be aware of what class of route a signalling message is about. (This information must be agreed between signalling application peers, and also exchanged with the NTLP.) This implies an extension to the API to the common layer in order to carry these indications, in some near-standardised syntax.

The standardised syntax of the second requirement must match the network capabilities of the first; one example is the extensions to MPLS of [24]. Once that extension is in place, the operation of the NTLP to invoke the underlying network appropriately seems to be mainly a node-internal (implementation) issue.

5. Security Considerations

Any redistribution of functionality within an architecture introduces new security problems and mitigates some old ones. However, the path-decoupled problem space discussed here mostly overlaps with the existing work being carried out within NSIS, since the interactions within and between signalling applications, and the interactions between signalling applications and other elements in the network, are mostly unchanged. The various centralisation options introduce extra node types into the picture, but probably reduce the overall number of them involved; it is not clear whether the net impact of these changes on network security is positive or negative, but it clearly depends mainly on the design of any new protocols required, which in turn depends on the ability to make sensible assumptions about what trust and authority relationships can be required between these nodes.
The other main technical difference between path-coupled and
decoupled signalling is that there are no longer well-defined
constraints on the topological path taken by the signalling messages
themselves. In the path-coupled case, these constraints can be used
to eliminate certain attacks by off-path nodes on the NTLP operation,
for example by ingress filtering. However, the strength of the
protection possible always depends on the physical and topological
characteristics of the network and is never perfect; most likely in
the path-decoupled case, their place would have to be taken by other
mechanisms. Details are for further study.

6. Conclusions

This draft has provided an overview of the problem space for path-
decoupled signalling in the NSIS problem space, including the
engineering motivations for such approaches and considerations of
scenarios where they may be applicable. It has also presented a
decomposition of the problem space into a set of component parts,
with some initial discussion for each of whether these require new
development or could be satisfied using existing protocols.

It is our conclusion that a small number of relatively precisely
scoped extensions to existing NSIS (in particular, NTLP)
functionality could be used to enhance the performance and usability
of the NSIS protocol suite in several important networking
environments, and in particular could ease deployment and
interworking with other networks that attach to the Internet. We
therefore recommend that the working group should consider taking on
this work.

7. References

7.1 Normative References

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

"Middlebox Communications (midcom) Protocol Requirements",
RFC 3304, August 2002.

[3] Chaskar, H., "Requirements of a Quality of Service (QoS)

7.2 Informative References


[15] 3GPP, "Architectural enhancements for end-to-end Quality of Service (QoS)", 3GPP TR 23.802 0.4.0, February 2005.


draft-ietf-pce-architecture-00 (work in progress), March 2005.


Authors’ Addresses

Robert Hancock
Siemens/Roke Manor Research
Old Salisbury Lane
Romsey, Hampshire  SO51 0ZN
UK

Email: robert.hancock@roke.co.uk

Cornelia Kappler
Siemens AG
Siemensdamm 62
13627 Berlin
Germany

Email: cornelia.kappler@siemens.com
Appendix A. Acknowledgements

Sven van den Bosch of Alcatel contributed to several sections of this draft.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.