Signaling Using the NSIS Framework; Messaging and End-host Mobility Applications

Teemu Huovila and Lauri Liuhto
University of Helsinki
{teemu.huovila, lauri.liuhto}@cs.helsinki.fi

May 15, 2007

We first briefly introduce the central aspects of a new approach to designing and developing signaling applications. Then we present two different applications, that are currently being developed using this common platform.

Next Steps In Signaling Framework

The Next Steps in Signaling (NSIS) working group of the Internet Engineering Task Force (IETF) has developed a two-layered design to facilitate signaling over IP networks, the NSIS Framework. It consists of the NSIS Transport Layer Protocol (NTLP) and NSIS Signaling Layer Protocols (NSLPs). This division is made to ease signaling application development by having a common transport mechanism that provides basic services, such as transport, to signaling applications. A realization of NTLP, called the General Internet Signaling Transport (GIST), is also proposed by the NSIS working group.

The four main services that GIST provides to NSLPs are:

Peer discovery In the NSIS Framework NSLPs are identified by a NSLP Identifier. GIST finds the next NSLP level hop.

Signaling transport GIST provides a signaling transport service. Two alternative transport modes exist, unreliable (D-mode) and reliable (C-mode). In D-mode UDP is used as a backend and TCP is used in C-mode.

Channel security GIST provides basic channel security services to signaling applications. These include message integrity and confidentiality protection together with protection against message injection and replay attacks.

API GIST provides a common API to NSLPs. All communications between NSLP and GIST is done via GIST NSLP API.

End-host Mobility Application

The end-host mobility application is a protocol designed and deployed as a NSLP. Each GIST node in the network, that provides the mobility feature, has to run the mobility protocol application. The task of the mobility protocol is to

manage per-host routing of Mobile Node (MN) traffic. The mobility protocol lets mobile nodes stay connected to each other and to outside networks.

The intended deployment environment for the mobility NSLP is a mesh access network with multiple gateways to outside networks. In mesh access networks mesh routers form densely interconnected multi-hop topologies, to provide client hosts connectivity. Links between routers can be either wired or wireless. It is assumed that, once the network is up and running, changes in the core topology and routing paths are less frequent. Still, routers may come and go at will. A functioning router-to-router forwarding is expected to be in place. In other words it is assumed, that the routers making up the mesh access network run some type of IP routing protocol to forward the traffic between them selves

In the mobility protocol *Edge Access Routers* (EARs) monitor network traffic to detect and facilitate movement of their client nodes. The EARs also put together `Info` messages about client nodes. All *Access Routers* (ARs) proactively exchange information, originating from the EARs, about client nodes. Handovers are triggered by client data packets or, if available, link-layer notifications or other cross-layer information. The triggering data is combined with the proactively exchanged client information, to achieve the handover.

Access Routers create data paths in the network to route data from the mobile nodes, that are disassociated from the topology of the network. Routes are created by `Set route` messages, that are sent by EARs, when a mobile node moves. A host route, i.e. with a prefix or netmask matching the route to a single destination host, is created for traffic from the MNs original section of the network, to its current location. In the other direction, for traffic from the MN, a source host route is set on intermediate routers. This means that traffic originating from the MN is forwarded based on the senders address.

The mobility NSLP uses symmetric routes by default. This means that routes are set for both inbound and outbound traffic. In many scenarios it would also be possible to use asymmetric routes, so that host routes are set only for inbound traffic and outbound is directed to the default mesh gateway of the current network. This would have the effect of reducing the overall round-trip time of the traffic, by optimizing the route for outbound packets, if the default mesh gateway is located closer. Symmetric routes were selected as a default for the mobility NSLP, since we expect that they will be more reliable in some scenarios. For example quality of service and firewall signaling protocols are designed with symmetric routes in mind.

Messaging NSLP

The new messaging protocol (Messaging NSLP) is going to be used to transfer messages between signaling nodes in a network. The main motivation to design this new protocol is the need to transfer monitoring information between routers, but it can be utilized also in other domains. While NSIS Framework makes signaling application development easier, some problems still exists. For example, NSLP identifiers are quite strictly managed. This fact alone makes it nearly impossible to create large amount of small signaling applications and creates a need for generic messaging service.

The Messaging NSLP itself is quite simple and it provides a simple API to Messaging Applications. The Messaging NSLP API consists of four opera-

tions, *open()*, *close()*, *read()* and *write()*. Messaging applications, identified by application identifier, access network resources through these four operations.

Example scenario where Messaging NSLP with battery and network link monitoring applications could be useful can be seen in Figure 1. On left side we have a mesh network of battery powered routers $R_1 \ldots R_3$ and three hosts $H_1 \ldots H_3$. Hosts H_1 and H_2 are communicating very actively, and router R_3 is running low on battery. Because routers are running battery and link load monitoring applications they can alter routing (right side of the figure 1). This change makes host H_3 possible to maintain network connection.

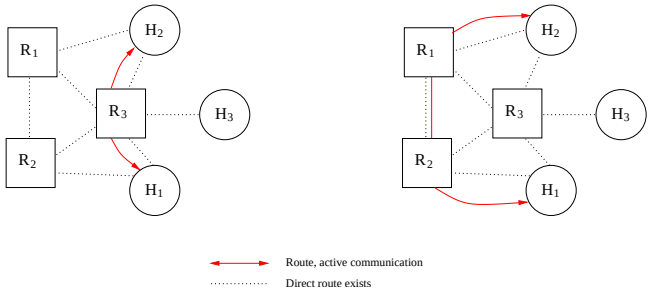

Figure 1: Battery and link load monitoring in mesh network

Future Work

Initial specifications for the presented signaling applications have been completed by the authors of this document. Work on implementing both of the specifications is on-going. Additionally an implementation of GIST is being worked on, at the University of Helsinki.