Quality-of-Service Signaling for Virtual Networks

Roland Bless and Martin Röhricht
Institute of Telematics
Karlsruhe Institute of Technology (KIT)
Zirkel 2, P.O.Box 6980, 76049 Karlsruhe, Germany
Email: {bless, roehricht}@kit.edu

I. Introduction

Network virtualization is a promising abstraction technique, not only to optimize the utilization of network resources, but also to design and actually bring out completely novel network architectures and protocols [1]. Such a virtual network consists of virtual nodes that are interconnected by virtual links. Thus the virtual network builds its own logical overlay structure on top of the physical "substrate", i.e. the underlying real physical network. Virtual links are, however, mostly configured statically, or do not provide Quality-of-Service (QoS) guarantees along the entire substrate path or are limited to a specific administrative domain. While there are lots of different link virtualization technologies in the substrate available (from Virtual LANs to MPLS LSPs), we consider in this paper an IP-based substrate as well as also inter-provider, inter-domain virtual links.

In order to setup and configure virtual links dynamically and on-demand between providers, signaling protocols are needed. The Internet Engineering Task Force's (IETF) Next Steps in Signaling (NSIS) framework already provides an up-to-date signaling protocol suite that can be used for various different signaling applications [2], e.g., for QoS resource reservations.

In our approach we combine the signaling for QoS guarantees (i.e., resource reservation) in the substrate with the virtual link setup signaling to reduce the time required for virtual link set up. In this paper, we examine how the NSIS QoS NSLP protocol can be extended in order to be used for virtual link signaling. We discuss the advantages of using a path-coupled signaling model as it is used by the QoS NSLP protocol. We then describe potential challenges and problems that arise in the context of virtual networks and provide a set of possible solutions.

II. The Next Steps in Signaling Protocols

The NSIS framework was designed within the IETF to provide a modern and generic Internet signaling protocol suite for various signaling applications. NSIS follows a two-layered architecture where the lower layer, called NSIS Transport Layer Protocol (NTLP) is responsible for the routing and transport of signaling messages. The *General Internet Signaling Transport* (GIST) protocol [3] is a concrete realization of an NTLP. The actual signaling application's logic is provided by a corresponding upper NSIS Signaling Layer Protocol (NSLP), e.g. *QoS NSLP* for QoS signaling [4].

GIST uses IPv4/IPv6 and already existing transport protocols, like UDP, TCP, TCP with TLS, or SCTP for signaling message transport. *Message Routing Methods (MRM)* define the routing algorithm for signaling messages. GIST uses a *path-coupled MRM* by default, where signaling messages follow strictly the data flow's path. This is achieved by sending the signaling packet to the data flow's IP destination address, while intermediate NSIS nodes intercept such signaling messages that they are interested in. This interception is realized by using a *Router Alert Option* of IP packets. This MRM proves especially advantageous with regard to QoS signaling, as it allows to install state within intermediate nodes along the data path and furthermore automatically detects and adapts to possible route changes.

III. Challenges of using Path-Coupled Signaling for Virtual Networks

Virtual networks consist of virtual nodes and virtual links, e.g. as depicted in Figure 1. *Virtual nodes* are usually realized by virtual machines running on a physical node and should be conceptually independent from the actual virtualization technology being used. *Virtual links* may also be realized by a variety of different substrate techniques, e.g. VLANs, MPLS or for IP-based substrate network various IP tunnels like IP-in-IP tunnel, Generic Routing Encapsulation (GRE), or L2TP tunnels. Usually, inside the virtual nodes other non IP-based network architectures are running. For the rest of the paper we assume an IP-based substrate and assume that an IP-based network architecture is also running inside a virtual node. The signaling control entity that sets up and maintains virtual links for virtual networks should operate decoupled from the virtual machines, i.e., a virtual machine (VM) should not need to provide a signaling control entity on its own. By using the NSIS signaling protocols to setup virtual links, we consider an NSIS control instance to be an appropriate control entity running inside a physical node.

As already stated above, *path-coupled signaling* proves advantageous for QoS resource reservations as it allows to install state in exactly those nodes that belong to the data flow's path. Furthermore, it is assured that a working path exists. Path-coupled signaling will work for any tunneled solution, i.e., the outer tunnel IP destination address is used as destination address for the signaling messages, that discover the signaling path. Tunneling, however, always includes encapsulation overhead. Especially when considering IPv6 as

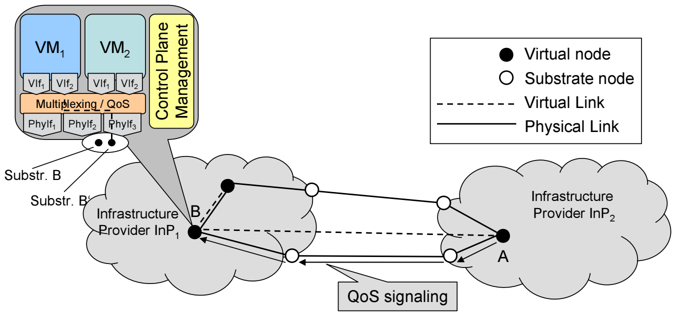

Figure 1. Overview of a virtual network model

substrate protocol, it is possible that a VM gets its own IP address, because there are 64 bit available for addressing hosts within a subnet. In this case the virtual link uses the VMs' IP address (cf. IP address B' in Fig. 1) and consequently path-coupled signaling would use it as destination address. This, however, poses some central challenges on a signaling protocol that should be used to setup virtual networks.

Signaling messages being addressed towards a VM that does run a signaling control entity inside, would simply not be able to create a signaling association between the two end-points. Such signaling messages should therefore be intercepted by the signaling control entity on the physical node instead. For instance, consider the situation depicted in Figure 2 where we want to establish a virtual link between VM$_P$, being equipped with a MAC address M$_P$ and an IP address IP$_P$ and VM$_Q$ with MAC address M$_Q$ and IP address IP$_Q$. VM$_P$ runs on node A that is addressed by M$_A$ and IP$_A$, whereas VM$_Q$ runs on node B that can be reached via M$_B$ and IP$_B$. In this setup a virtual link should span a path between IP$_P$ and IP$_Q$. However, how can be assured, that physical node B intercepts these signaling messages on behalf of VM$_Q$? How can signaling messages for IP$_B$ be processed by the signaling control entity in node B?

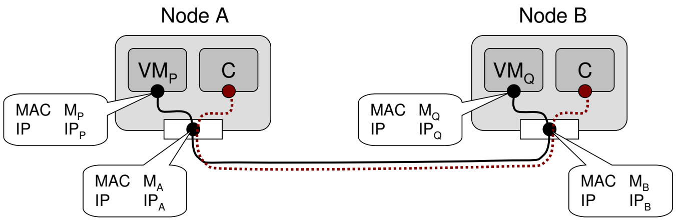

Figure 2. Challenges for the use of the path-coupled signaling model in a virtual network environment

In the following we propose a set of possible solutions how path-coupled signaling may be used for virtual link setups and discuss advantages and limitations of each presented approach.

A. Explicit signaling target MRM

Instead of relying on a path-coupled MRM, we could also use a so-called Explicit Signaling Target MRM [5]. This MRM can be used to directly send signaling messages towards an explicitly addressed entity. In the example provided above, signaling messages from the control entity in node A should be addressed by an EST-MRM towards IP$_B$. However, signaling would not be performed in a path-coupled manner so that state for QoS reservations cannot be installed in intermediate nodes that are located on the actual data path.

B. Using packet classifiers

In a different approach signaling messages are sent path-coupled for an "outer flow" from node A to node B that install state for an "inner flow" from IP$_A$ to IP$_B$ by means of a specific packet classifier. This results in signaling messages being exchanged between the NSIS control entities only, while state for the data path can be installed. However, this may also not be strictly path-coupled in cases where routing for the substrate and packet classifier differs.

C. Router Alert Option codepoint

Special code points for the router alert option may be used for reservation aggregates. This may also be considered as a valid approach in order to let signaling messages being addressed for the virtual machine but being intercepted by the NSIS control entity. However, this router alert option must then be explicitly supported by the intermediate nodes participating in this signaling session.

D. GIST Header Flag Extension

The most promising approach is to introduce a new GIST header flag and use some sort of deep packet inspection. This GIST header flag allows for the interception of an NSIS control entity on behalf of a virtual machine running on the same physical machine. The NSIS control entity must then know that it is (a) responsible to intercept messages with this particular header flag on behalf of someone else, and (b) must be configured on behalf of which virtual machines it acts.

IV. Conclusion

We presented the idea to couple QoS signaling with virtual link setup. Path-couped signaling is advantageous, because the actual substrate path is traversed and verified to function. In case the virtual nodes are not using tunneling, but get their own assigned IP addresses, path-coupled signaling is not easily possible anymore. We sketched potential solutions and briefly discussed their pros and cons. Currently, we are implementing some of the potential solutions in order to compare their performance.

References

[1] A. Feldmann, M. Kind, O. Maennel, G. Schaffrath, and C. Werle, "Network Virtualization - An Enabler for Overcoming Ossification," *Ercim News*, pp. 21–22, Apr. 2009, Invited Article.

[2] X. Fu, H. Schulzrinne, A. Bader, D. Hogrefe, C. Kappler, G. Karagiannis, H. Tschofenig, and S. V. den Bosch, "NSIS: A New Extensible IP Signaling Protocol Suite," *Communications Magazine, IEEE*, vol. 43, no. 10, pp. 133–141, Oct. 2005.

[3] H. Schulzrinne and R. Hancock, "GIST: General Internet Signalling Transport," http://tools.ietf.org/id/draft-ietf-nsis-ntlp, IETF, Jun. 2009, Internet Draft draft-ietf-nsis-ntlp-20.

[4] J. Manner, G. Karagiannis, and A. McDonald, "NSLP for Quality-of-Service Signaling," http://tools.ietf.org/id/draft-ietf-nsis-qos-nslp, IETF, Jan. 2010, Internet Draft draft-ietf-nsis-qos-nslp-18.

[5] R. Bless, "An Explicit Signaling Target Message Routing Method (EST-MRM) for the General Internet Signaling Transport (GIST) Protocol," http://tools.ietf.org/html/draft-bless-nsis-est-mrm-02, IETF, Jun. 2010, Internet-Draft draft-bless-nsis-est-mrm-02.txt (Work in progress).