6man Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 3, 2012

S. Krishnan
A. Kavanagh
B. Varga
Ericsson
S. Ooghe
Alcatel-Lucent
E. Nordmark
Cisco

March 2, 2012

The Line Identification Destination Option
draft-ietf-6man-lineid-03

Abstract

In Ethernet based aggregation networks, several subscriber premises may be logically connected to the same interface of an edge router. This document proposes a method for the edge router to identify the subscriber premises using the contents of the received Router Solicitation messages. The applicability is limited to broadband network deployment scenarios where multiple user ports are mapped to the same virtual interface on the Edge Router.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 3, 2012.

Table of Contents

1. Introduction

Digital Subscriber Line (DSL) is a widely deployed access technology for Broadband Access for Next Generation Networks. While traditionally DSL access networks were Point-to-Point Protocol (PPP) [RFC1661] based some networks are migrating from the traditional PPP access model into a pure IP-based Ethernet aggregated access environment. Architectural and topological models of an Ethernet aggregation network in context of DSL aggregation are described in [TR101].

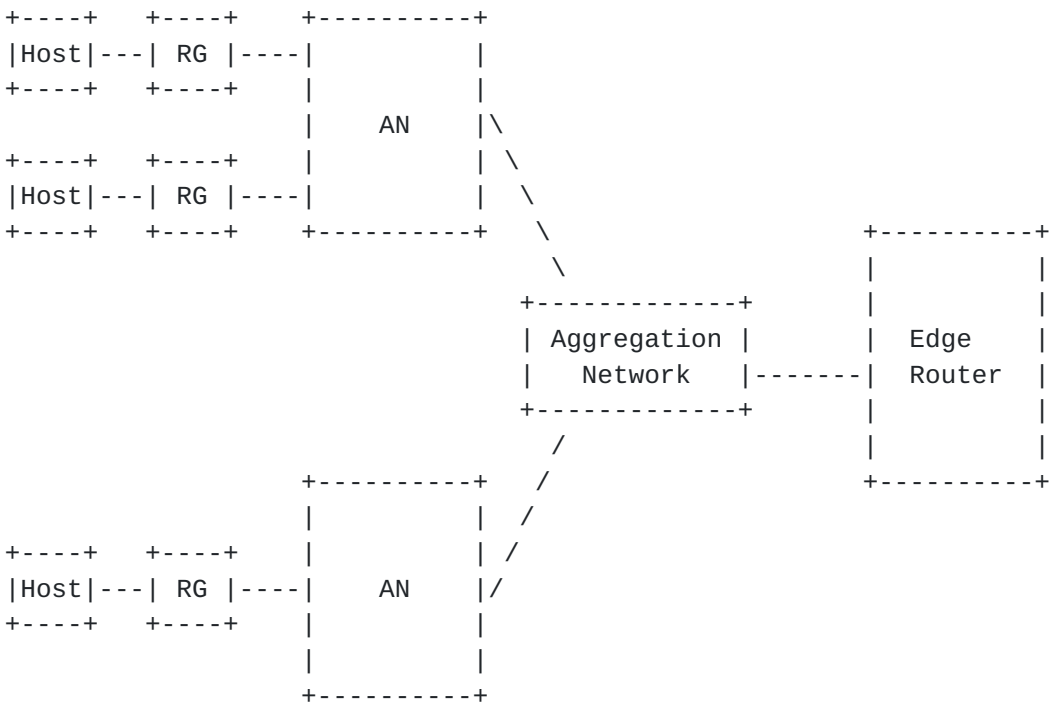

Figure 1: Broadband Forum Network Architecture

One of the Ethernet and GPON aggregation models specified in this document bridges sessions from multiple user ports behind a DSL Access Node (AN), also referred to as a Digital subscriber line access multiplexer (DSLAM), into a single VLAN in the aggregation network. This is called the N:1 VLAN allocation model.

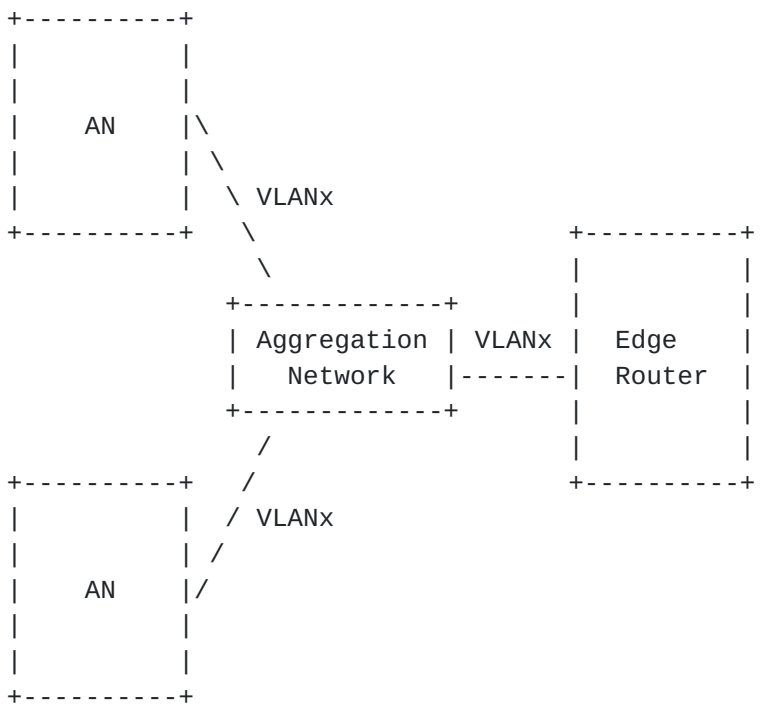

Figure 2: n:1 VLAN model

1.1. Terminology

1:1 VLAN	It is a broadband network deployment scenario where each user port is mapped to a different VLAN on the Edge Router. The uniqueness of the mapping is maintained in the Access Node and across the Aggregation Network.
N:1 VLAN	It is a broadband network deployment scenario where multiple user ports are mapped to the same VLAN on the Edge Router. The user ports may be located in the same or different Access Nodes.
AN	A DSL or a Gigabit Passive Optical Network (GPON) Access Node. The Access Node terminates the physical layer (e.g. DSL termination function or GPON termination function), may physically aggregate other nodes implementing such functionality, or may perform both functions at the same time. This node contains at least one standard Ethernet interface that serves as its "northbound" interface into which it aggregates traffic from several user ports or Ethernet-based "southbound" interfaces.

	It does not implement an IPv6 stack but performs some limited inspection/ modification of IPv6 packets. The IPv6 functions required on the Access Node are described in Section 5 of [TR177].
Aggregation Network	The part of the network stretching from the Access Nodes to the Edge Router. In the context of this document the aggregation network is considered to be Ethernet based, providing standard Ethernet interfaces at the edges, for connecting the Access Nodes and Broadband Network. It is comprised of ethernet switches that provide very limited IP functionality (e.g. IGMP snooping, MLD snooping etc.).
Edge Router	The Edge Router, also known as the Broadband Network Gateway (BNG) is the first IPv6 hop for the user. In the cases where the RG is bridged, the BNG acts as the default router for the hosts behind the RG. In cases where the RG is routed, the BNG acts as the default router for the RG itself. This node implements IPv6 router functionality.
GPON	Gigabit-capable Passive Optical Network is an optical access network that has been introduced into the Broadband Forum architecture in [TR156]
Host	A node that implements IPv6 host functionality.
RG	A residential gateway device. It can be a Layer 3 (routed) device similar to one specified in or a Layer 2 (bridged) device. The residential gateway for Broadband Forum networks is defined in [TR124]
End-device	A node that sends Router Solicitations and processes received Router Advertisements. When a Layer 3 RG is used it is considered an end-device in the context of this document. When a Layer 2 RG is used, the host behind the RG is considered to be an end-device in the context of this document.

1.2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Applicability Statement

The line identification destination option is intended to be used only for the N:1 VLAN deployment model. For the other VLAN deployment models line identification can be achieved differently.

When DHCP is used for IPv6 address assignment it has the side-effect of including reliability initiated by the end-device (the end-device retransmits DHCP messages until it receives a response), as well as a way to detect when the end-device is not active for an extended period of time (the end-device would not renew its DHCP lease). IPv6 Stateless address autoconfiguration was not designed to satisfy such requirements. While this protocol improves the the robustness of relying on Router Solicitations in lieu of DHCP, this results on some limitations specified below.

The mechanism described in this document deals with the loss of subscriber-originated Router Solicitations by initiating RSs at the Access Node, which improves the robustness over solely relying on the end-device's few initial retransmissions of RSs. But the AN retransmissions imply that some information that was obtained by the network from subscriber-originated RSs may no longer be available. e.g. Since there is no L2 frame received from the subscriber in case of an RS sent by an AN, the L2 address information of the host cannot be determined. One piece of L2 address information currently used in Broadband networks is the MAC address. For this reason, the solution described in this document is NOT RECOMMENDED for networks that require the MAC address of the endpoint for identification.

There is no indication when a subscriber is no longer active. Thus this protocol can not be used to automatically reclaim resources, such as prefixes, that are associated with an active subscriber. See Section 8. Thus this protocol is NOT RECOMMENDED for networks that require automatic notification when a subscriber is no longer active.

This mechanism by itself provides no protection against the loss of RS induced state in access routers that would lead to loss of IPv6 connectivity for hosts. Given that regular IPv6 hosts do not have RS retransmission behavior that would allow automatic recovery from such a failure, this mechanism is considered experimental and NOT RECOMMENDED for general deployments.

3. Issues with identifying the subscriber in an N:1 VLAN model

In a DSL or GPON based fixed Broadband Network, IPv6 end-devices are connected to an Access Node (AN). These end-devices today will typically send a Router Solicitation Message to the Edge Router, to

which the Edge Router responds with a Router Advertisement message. The Router Advertisement typically contains a prefix that the end-devices will use to automatically configure an IPv6 Address. Upon sending the Router Solicitation message the node connecting the end-device on the access circuit, typically an Access Node (AN), would forward the RS to the Edge Router upstream over a switched network. However, in such Ethernet-based aggregation networks, several subscriber premises may be connected to the same interface of an edge router (e.g. on the same VLAN). However, the edge router requires some information to identify the end-device on the circuit the end-device is connected on. To accomplish this, the AN needs to add line identification information to the Router Solicitation message and forward this to the Edge Router. This is analogous to the case where DHCP is being used, and the line identification information is inserted by a DHCP relay agent. This document proposes a method for the edge router to identify the subscriber premises using the contents of the received Router Solicitation messages.

4. Basic operation

This document recommends tunneling Neighbor discovery packets inside another IPv6 packet that uses a destination option to convey line identification information. The Neighbor discovery packets are left unmodified inside the encapsulating IPv6 packet. In particular, the Hop Limit field of the ND message is not decremented when the packet is being tunneled. This is because ND messages whose Hop Limit is not 255 will be discarded by the receiver of such messages.

5. Access Node Behavior

5.1. On receiving a Router Solicitation from the end-device

When an end-device sends out a Router Solicitation, it is received by the access node. The AN identifies these messages by looking for ICMPv6 messages (IPv6 Next Header value of 58) with ICMPv6 type 133. The AN intercepts and then tunnels the received Router Solicitation in a newly created IPv6 datagram with the Line Identification Option (LIO). The AN forms a new IPv6 datagram whose payload is the received Router Solicitation message as described in [RFC2473] except that the Hop Limit field of the Router Solicitation message MUST NOT be decremented. If the AN has an IPv6 address, it SHOULD use this address in the Source Address field of the outer IPv6 datagram. Otherwise it MUST use the unspecified address as the Source Address of the outer IPv6 datagram. The destination address of the outer IPv6 datagram MUST be copied from the destination address of the tunneled RS. The AN MUST insert a destination options header between

the outer IPv6 header and the payload. It MUST insert a LIO destination option and set the line identification field of the option to contain the circuit identifier corresponding to the logical access loop port of the Access Node from which the RS was initiated.

5.2. On receiving a Router Advertisement from the Edge Router

When the edge router sends out a tunneled router advertisement in response to the RS, it is received by the access node. If there is an LIO option present, the AN MUST use the line identification data of the LIO option to identify the subscriber agent circuit of the Access Node on which the RA should be sent. The AN MUST then remove the outer IPv6 header of this tunneled RA and multicast the inner packet (the original RA) on this specific subscriber circuit.

5.2.1. Identifying tunneled Router Advertisements

The Access Node can identify tunneled RAs by installing filters based on the destination address (All BBF Access Nodes) of the outer packets, and the presence of a destination option header with an LIO destination option.

5.3. On detecting a subscriber circuit coming up

RSs initiated by end-devices as described in Section 5.1 may be lost due to lack of connectivity between the access node and the end-device. To ensure that the end-device will receive an RA, the AN needs to trigger the sending of periodic RAs on the edge router. For this purpose, the AN needs to inform the edge router that a subscriber circuit has come up. When the access node detects that a subscriber circuit has come up, it MUST create a Router Solicitation message as described in Section 6.3.7 of [RFC4861]. It MUST use the unspecified address as the source address of this RS. It MUST then tunnel this RS towards the edge router as described in Section 5.1.

In case there are connectivity issues between the AN and the edge router, the RSs initiated by the AN can be lost. The AN SHOULD continue retransmitting the Router Solicitations following the algorithm described in Section 5.5 for a given LIO until it receives an RA for that specific LIO.

5.4. On detecting Edge Router failure

When the edge router reboots and loses state or is replaced by a new edge router, the AN will detect it using connectivity check mechanisms that are already in place in Broadband networks (e.g. BFD). When such edge router failure is detected, the AN needs to start transmitting RSs for each of its subscriber circuits that are

up as described in Section 5.3.

5.5. RS Retransmission algorithm

The AN SHOULD use the exponential backoff algorithm for retransmits that is described in Section 14 of [RFC3315] in order to continuously retransmit the Router Solicitations for a given LIO until a response is received for that specific LIO. The AN SHOULD use the following variables as input to the retransmission algorithm:

```
IRT  1 Second
MRT  30 Seconds
MRC  0
MRD  0
```

6. Edge Router Behavior

6.1. On receiving a Tunneled Router Solicitation from the Access Node

When the edge router receives a tunneled Router Solicitation forwarded by the access node, it needs to check if there is an LIO destination option present in the outer datagram. The edge router can use the contents of the line identification field to lookup the addressing information and policy that need to be applied to the line from which the Router Solicitation was received. The edge router MUST then process the inner RS message as specified in [RFC4861]

6.2. On sending a Router Advertisement towards the end-device

When the edge router sends out a Router Advertisement in response to a tunneled RS that included an LIO option, it MUST tunnel the Router Advertisement in a newly created IPv6 datagram with the Line Identification Option (LIO). The edge router creates the Router Advertisement message as described in Section 6.2.3 of [RFC4861]. The edge router may use the contents of the LIO in the received router solicitation to determine the contents of this router advertisement(es. The Edge Router then forms a new IPv6 datagram, whose payload is the Router Advertisement message, as described in [RFC2473] except that the Hop Limit field of the Router Advertisement message MUST NOT be decremented. The Edge router MUST use a link-local IPv6 address on the outgoing interface in the Source Address field of the outer IPv6 datagram. The destination address of the outer IPv6 datagram MUST be set to the well-known link-local scope All BBF Access Nodes multicast address [to be allocated]. The edge router MUST insert a destination options header between the outer IPv6 header and the payload. It MUST insert a LIO destination option and set the line identification field of the option to contain the

circuit identifier corresponding to the logical access loop port of the Access Node to which the RA MUST be sent. The IPv6 destination address of the inner RA MUST be set to the all-nodes multicast address. The link-layer destination address of the tunneled RA MUST be set to the unicast link-layer address of the Access Node that sent the tunneled Router Solicitation which is being responded to.

6.3. Sending periodic unsolicited Router Advertisements towards the end-device

After sending a tunneled Router Advertisement as specified in Section 6.2 in response to a received RS, the edge router MUST store the mapping between the LIO and the prefixes contained in the Router Advertisement. It should then initiate periodic sending of unsolicited Router Advertisements as described in Section 6.2.3. of [RFC4861] . The Router Advertisements MUST be created and tunneled as described in Section 6.2. The edge router MAY stop sending Router Advertisements if it receives a notification from the AN that the subscriber circuit has gone down. This notification can be received out-of-band using a mechanism such as ANCP.

7. Line Identification Destination Option (LIO)

The Line Identification Destination Option (LIO) is a destination option that can be included in IPv6 datagrams that tunnel Router Solicitation and Router Advertisement messages. Multiple Line Identification destination options MUST NOT be present in the same IPv6 datagram. The LIO has an alignment requirement of (none).

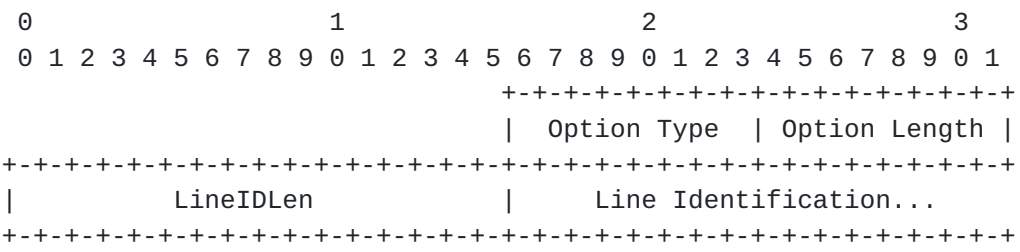

Figure 3: Line Identification Destination Option Layout

Option Type

8-bit identifier of the type of option. The option identifier for the line identification option will be allocated by the IANA.

Option Length

8-bit unsigned integer. The length of the option (excluding the Option Type and Option Length fields). The value 0 is considered invalid.

LineIDLen

Length of the Line Identification field in number of octets.

Line Identification

Variable length data inserted by the Access Node describing the subscriber agent circuit identifier corresponding to the logical access loop port of the Access Node from which the RS was initiated. The line idenfication should be encoded as specified in Section 7.1.

7.1. Encoding of Line ID

This IPv6 Destination Option is derived from an existing widely deployed DHCPv6 Option [RFC4649], which is in turn derived from a widely deployed DHCPv4 Option [RFC3046]. Both of those derive from and cite the basic DHCP options specification [RFC2132]. Those widely deployed DHCP options use the NVT character set [RFC2132][RFC0020]

The IPv6 Line ID option contains a description which identifies the line, using only character positions (decimal 32 to decimal 126, inclusive) of the US-ASCII character set [X3.4], [RFC0020]. Consistent with [RFC2132], [RFC3046] and [RFC4649], the Line ID field SHOULD NOT contain the US-ASCII NUL character (decimal 0). However, implementations receiving this option MUST NOT fail merely because an ASCII NUL character is (erroneously) present in the Line ID option's data field.

Some existing widely deployed implementations of edge routers and access nodes that support the previously mentioned DHCP option only support US-ASCII, and strip the high-order bit from any 8-bit characters entered by the device operator. The previously mentioned DHCP options do not support 8-bit character sets either. Therefore, for compatibility with the installed base and to maximise

interoperability, the high-order bit of each octet in this field MUST be set to zero by any device inserting this option in an IPv6 packet.

Consistent with [RFC3046] and [RFC4649], this option always uses binary comparison. Therefore, two Line IDs MUST be equal when they match when compared byte-by-byte. Line-ID A and Line-ID B match byte-by-byte when (1) A and B have the same number of bytes and (2) for all byte indexes P in A: the value of A at index P has the same binary value as the value of B at index P.

Two Line IDs SHOULD NOT be equal if they do not match byte-by-byte. For example, an IPv6 Line ID option containing "f123" is not equal to a Line ID option "F123".

Intermediate systems SHOULD NOT examine the contents of the Line ID. Intermediate systems SHOULD NOT alter the contents of the Line ID.

8. Garbage collection of unused prefixes

Following the mechanism described in this document, the Broadband network associates a prefix to a subscriber line based on the LIO. Even when the subscriber line goes down temporarily, this prefix stays allocated to that specific subscriber line. i.e. The prefix is not returned to the unused pool. When a subscriber line no longer needs a prefix, the prefix can be reclaimed by manual action dissociating the prefix from the LIO in the backend systems.

9. Interactions with Secure Neighbor Discovery

Since the SEND [RFC3971] protected RS/RA packets are not modified in anyway by the mechanism described in this document, there are no issues with SEND verification.

10. Acknowledgements

The authors would like to thank Margaret Wasserman, Mark Townsley, David Miles, John Kaippallimalil, Eric Levy-Abegnoli, Thomas Narten, Olaf Bonness, Thomas Haag, Wojciech Dec, Brian Haberman, Ole Troan, Hemant Singh, Jari Arkko, Joel Halpern, Bob Hinden, Ran Atkinson and Glen Turner for reviewing this document and suggesting changes.

11. Security Considerations

The line identification information inserted by the access node or

the edge router is not protected. This means that this option may be modified, inserted, or deleted without being detected. In order to ensure validity of the contents of the line identification field, the network between the access node and the edge router needs to be trusted.

12. IANA Considerations

This document defines a new IPv6 destination option for carrying line identification. IANA is requested to assign a new destination option type in the Destination Options registry maintained at

http://www.iana.org/assignments/ipv6-parameters

<TBA1> Line Identification Option [RFCXXXX]

The act bits for this option need to be 10 and the chg bit needs to be 0.

This document also requires the allocation of a well-known link-local scope multicast address from the IPv6 Multicast Address Space Registry located at

http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml

<TBA2> All BBF Access Nodes [RFCXXXX]

13. References

13.1. Normative References

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure

Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[TR101] Broadband Forum, "Migration to Ethernet-based DSL aggregation", <http://www.broadband-forum.org/technical/download/TR-101.pdf>.

[TR124] Broadband Forum, "Functional Requirements for Broadband Residential Gateway Devices", <http://www.broadband-forum.org/technical/download/TR-124_Issue-2.pdf>.

[TR156] Broadband Forum, "Using GPON Access in the context of TR-101", <http://www.broadband-forum.org/technical/download/TR-156.pdf>.

[TR177] Broadband Forum, "IPv6 in the context of TR-101", <www.broadband-forum.org/technical/download/TR-177.pdf>.

[X3.4] American National Standards Institute, "American Standard Code for Information Interchange (ASCII)", Standard X3.4 , 1968.

13.2. Informative References

[RFC0020] Cerf, V., "ASCII format for network interchange", RFC 20, October 1969.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, August 2006.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Blvd Decarie
Town of Mount Royal, Quebec
Canada

Email: suresh.krishnan@ericsson.com

Alan Kavanagh
Ericsson
8400 Blvd Decarie
Town of Mount Royal, Quebec
Canada

Email: alan.kavanagh@ericsson.com

Balazs Varga
Ericsson

Email: balazs.a.varga@ericsson.com

Sven Ooghe
Alcatel-Lucent
Copernicuslaan 50
2018 Antwerp,
Belgium

Phone:
Email: sven.ooghe@alcatel-lucent.com

Erik Nordmark
Cisco
510 McCarthy Blvd.
Milpitas, CA, 95035
USA

Phone: +1 408 527 6625
Email: nordmark@cisco.com