

6man Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 24, 2011

S. Krishnan
A. Kavanagh
B. Varga
Ericsson
S. Ooghe
Alcatel-Lucent
E. Nordmark
Oracle
September 20, 2010

Line identification in IPv6 Router Solicitation messages
draft-krishnan-6man-rs-mark-08

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 the N:1 VLAN allocation model.

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 March 24, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft

Line Identification in RS

September 2010

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Terminology	4
1.2.	Conventions used in this document	5
2.	Issues with identifying the subscriber in an N:1 VLAN model .	6
3.	Applicability	6
4.	Basic operation	6
5.	Access Node Behavior	6
5.1.	On receiving a Router Solicitation from the end-device . .	6
5.2.	On receiving a Router Advertisement from the Edge Router	7
5.2.1.	Identifying tunneled Router Advertisements	7
5.3.	On detecting a subscriber circuit coming up	7
6.	Edge Router Behavior	8
6.1.	On receiving a Tunneled Router Solicitation from the Access Node	8
6.2.	On sending a Router Advertisement towards the end-device	8
6.3.	Sending periodic unsolicited Router Advertisements towards the end-device	8
7.	Line Identification Destination Option (LIO)	9
8.	Interactions with Secure Neighbor Discovery	10
9.	Acknowledgements	10
10.	Security Considerations	10
11.	IANA Considerations	11
12.	Normative References	11
	Authors' Addresses	11

1. Introduction

DSL is a widely deployed access technology for Broadband Access for Next Generation Networks. While traditionally DSL access networks were PPP 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].

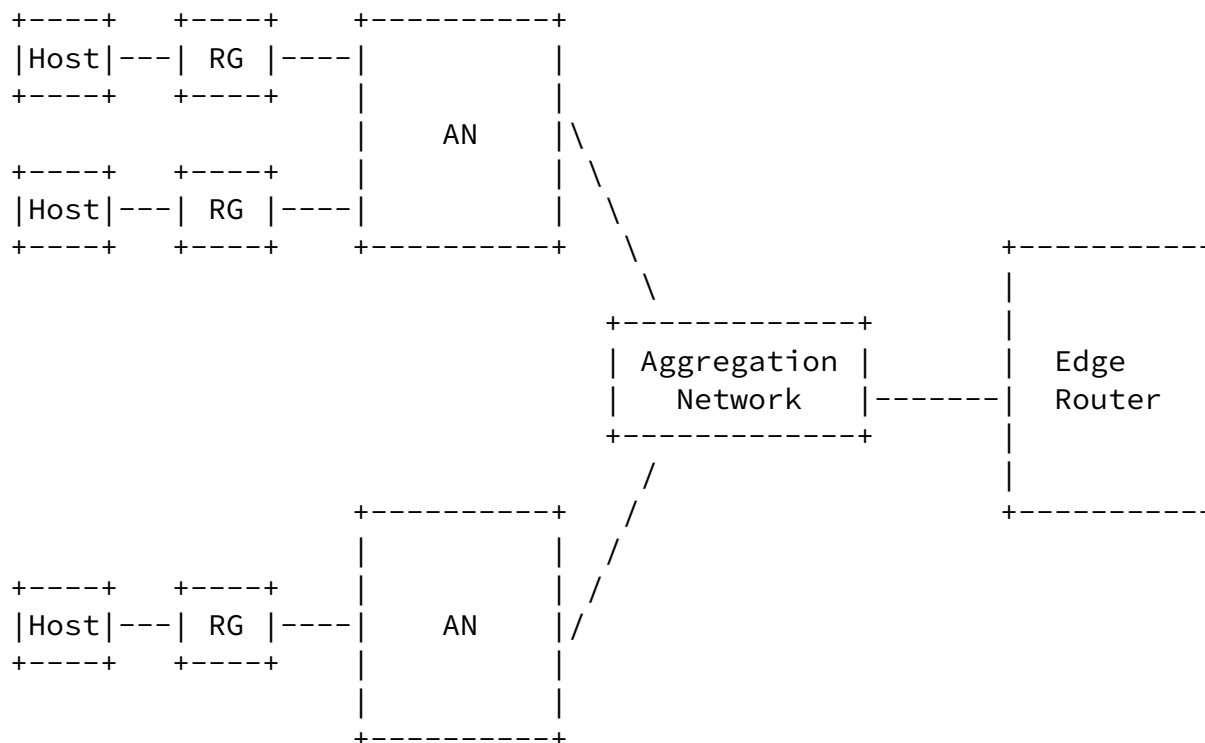


Figure 1: Broadband Forum Network Architecture

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 DSLAM, into a single VLAN in the aggregation network. This is called the N:1 VLAN allocation model.

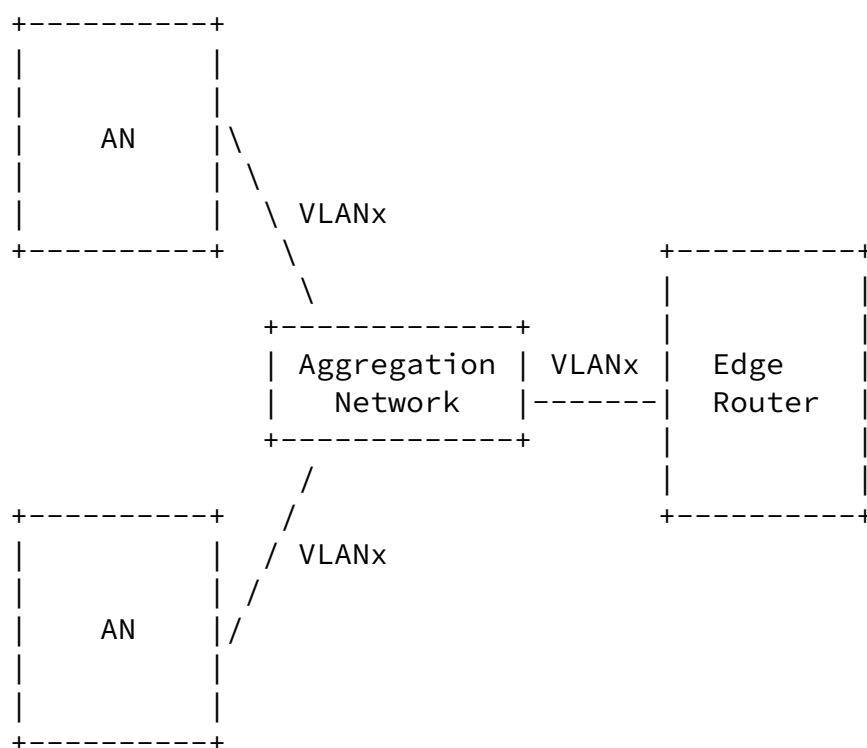


Figure 2: n:1 VLAN model

[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 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

Krishnan, et al.

Expires March 24, 2011

[Page 4]

Internet-Draft

Line Identification in RS

September 2010

	performs some limited inspection/modification of IPv6 packets.
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.](#) 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.

[3.](#) Applicability

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.

[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 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 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 RSeS initiated by the AN can be lost. The AN MAY continue retransmitting the Router Solicitations for a given LIO until it receives an RA for that specific LIO.

Alternately, the AN can send this notification about the subscriber

circuit coming up using a out-of-band mechanism with acknowledgements like ANCP, if such mechanism is available.

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 [KNOWN_VALUE_X, say fe80::0] . 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

7. Line Identification Destination Option (LIO)

[illegible]

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.

[8.](#) 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.

[9.](#) 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 and Joel Halpern for reviewing this document and suggesting changes.

10. 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.

Krishnan, et al.

Expires March 24, 2011

[Page 10]

Internet-Draft

Line Identification in RS

September 2010

11. 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>

<TBA> Line Identification Option [RFCXXXX]

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

12. Normative References

- [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.
- [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>>.

Krishnan, et al.

Expires March 24, 2011

[Page 11]

Internet-Draft

Line Identification in RS

September 2010

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
Oracle
17 Network Circle
Menlo Park, CA 94025
USA

Email: erik.nordmark@oracle.com