Workgroup: Network Working Group
Internet-Draft:
draft-carpenter-anima-l2acp-scenarios-02
Published: 9 April 2020
Intended Status: Informational
Expires: 11 October 2020
Authors: B. E. Carpenter Univ. of Auckland
B. Liu Huawei Technologies

Scenarios and Requirements for Layer 2 Autonomic Control Planes

Abstract

This document discusses scenarios and requirements for Autonomic Control Planes (ACPs) constructed and secured at Layer 2. These would be alternatives to an ACP constructed and secured at the network layer. A secure ACP is required as the substrate for an autonomic network and for the Generic Autonomic Signaling Protocol (GRASP).

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 https://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 11 October 2020.

Table of Contents

1. Introduction

As defined in [I-D.ietf-anima-reference-model], the Autonomic Service Agent (ASA) is the atomic entity of an autonomic function, and it is instantiated on autonomic nodes. When ASAs communicate with each other, they should use the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp]. It is essential that such communication is strongly secured to avoid malicious interference with the Autonomic Network Infrastructure (ANI).

For this reason, GRASP, and any other autonomic management traffic, must run over a secure substrate that is isolated from regular data plane traffic. This substrate is known as the Autonomic Control Plane (ACP). A method for constructing an ACP at the network layer is described in [I-D.ietf-anima-autonomic-control-plane]. The present document discusses scenarios and requirements for constructing an ACP at layer 2. It is not intended to be a normative specification, since implementation details will depend on individual layer 2 technologies.

2. Network Scenarios Suitable for a Layer 2 ACP

The ANI design is aimed at managed networks, as explained in the reference model [I-D.ietf-anima-reference-model]. For a wide area network (such as a large campus, a multi-site enterprise network, or a carrier network considered as a whole) it is appropriate to construct the ACP using network layer techniques and network layer security, which is the model described in [I-D.ietf-anima-autonomic-control-plane]. However, in at least two cases an ACP covering a smaller geographical area may be appropriate:

1. A small enterprise that is completely within one building or several adjacent buildings, which also requires autonomic network management.

2. An enterprise that prefers in any case to segment its network into smaller units for management purposes.

In either case, we assume that the L2 ACP may extend into the Network Operations Centre (NOC) so that it can be interfaced to traditional tools for Operations, Administration and Maintenance, as described in [RFC8368]. In the terminology of that document, an L2 ACP is an instance of a Generalized ACP.

3. Requirements for a Layer 2 Technology

These requirements are intended to ensure that a layer 2 ACP can meet the needs of all components of the ANI.

1. Since GRASP is specified to run over IPv6, the technology must support transmission of IPv6 packets according to [RFC8200]. Since GRASP can run on a single network segment using link-local addresses, there is not required to be an IPv6 router or DHCPv6 server.

2. The technology must support multicast. If the switches are not completely transparent to layer 2 multicast, they must support Multicast Listener Discovery Version 2 (MLDv2) for IPv6 [RFC3810].

3. The technology should have a minimum MTU of 1500 bytes. Note that since GRASP is specified to run unicast operations over TCP, this is not an absolute requirement and the IPv6 minimum MTU of 1280 bytes would be acceptable. GRASP UDP multicast messages could in principle be fragmented but in normal operation this would be unusual.

4. The technology must support isolation of a given set of nodes (the "ACP VLAN").

5. The technology must support secure authorization for access to the ACP VLAN. If the VLAN technology in use does not support password protection, a VLAN access control list could be used.

6. The technology should support both the normal dataplane VLAN and the ACP VLAN on the same physical sockets. (Possibly the dataplane may be the native VLAN, i.e. frames with no VLAN tag.)

7. The technology should support line speed encryption of the ACP VLAN.

8. The technology should support wired/wireless bridging if relevant.

9. The technology should require minimal manual configuration of ACP nodes. However, it is expected that the nodes will need to be preconfigured before deployment with the VLAN ID, and with a password or encryption key if necessary. A solution which is both secure and self-configuring at Layer 2 is out of scope for this document.

A specific security protocol that supports both authentication and encryption of layer 2 packets for Ethernet LANs is MACsec, i.e. the IEEE Standard 802.1AE-2018 [MACsec]. For multicast packets, authentication is on a group basis (i.e., the originator is guaranteed to be a member of the group, rather than a specific interface). MACsec applies across all VLANs, but the ACP VLAN can be isolated from the data plane VLAN independently of MACsec. This solution does not extend to wireless networks. For IEEE 802.11 networks, IEEE Standard 802.11-2016 [WiFi] "WPA2" security within a dedicated Basic Service Set (BSS) might be considered adequate.

An ACP software module will be needed in each autonomic node, whose job is to provide the GRASP core or other autonomic management protocols with the following information about the L2 ACP:

1. A signal that the L2 ACP is available and secure.

2. The current global scope IPv6 address that GRASP should use as its primary locator, preferably a ULA, if available. As mentioned, if no such address is available, GRASP will simply operate with link-local addresses.

3. A list of [interface_index, link_local_address] pairs for all valid IPv6 interfaces attached to the L2 ACP. The interface index (also known as a zone index [RFC4007]) is an integer for maximum portability between operating systems.

4. Multiple Segments

The L2 ACP could in principle be extended across multiple segments or even multiple sites by use of secure L2VPN technology. This topic is out of the scope of the present document.

5. Implementation Status [RFC Editor: please remove]

A simple ACP software module emulating that needed for a secure L2 ACP has been implemented, but it does not in fact verify security. It may be found at https://github.com/becarpenter/graspy/blob/master/acp.py and is briefly documented in https://github.com/becarpenter/graspy/blob/master/graspy.pdf.

6. Security Considerations

The assumption of this document is that any Layer 2 solution chosen must have adequate security against interlopers and eavesdroppers. It should be noted that (at least in a wired network) this also requires adequate physical security to prevent access by unauthorized persons, including physical intrusion detection.

The fact that an IPv6 router is not required in an L2 ACP excludes many Layer 3 vulnerabilities by construction. No outside entity can generate link-local IPv6 packets, and no outside entity can send global scope packets to any autonomic node.

7. IANA Considerations

This document makes no request of the IANA.

8. Acknowledgements

Excellent suggestions were made by Michael Richardson and other participants in the ANIMA WG.

9. References

9.1. Normative References

[MACsec] "IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Security", IEEE Standard 802.1AE-2018, 2018, <https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4007]
Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, DOI 10.17487/RFC4007, March 2005, <https://www.rfc-editor.org/info/rfc4007>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[WiFi] "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Standard 802.11-2016, 2016, <http://standards.ieee.org/getieee802/download/80211-2016.pdf>.

9.2. Informative References

[I-D.ietf-anima-autonomic-control-plane]
Eckert, T., Behringer, M., and S. Bjarnason, "An Autonomic Control Plane (ACP)", Work in Progress, Internet-Draft, draft-ietf-anima-autonomic-control-plane-24, 9 March 2020, <https://tools.ietf.org/html/draft-ietf-anima-autonomic-control-plane-24>.

[I-D.ietf-anima-grasp] Bormann, C., Carpenter, B., and B. Liu, "A Generic Autonomic Signaling Protocol (GRASP)", Work in Progress, Internet-Draft, draft-ietf-anima-grasp-15, 13 July 2017, <https://tools.ietf.org/html/draft-ietf-anima-grasp-15>.

[I-D.ietf-anima-reference-model]
Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", Work in Progress, Internet-Draft, draft-ietf-anima-reference-model-10, 22 November 2018, <https://tools.ietf.org/html/draft-ietf-anima-reference-model-10>.

[RFC8368] Eckert, T., Ed. and M. Behringer, "Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)", RFC 8368, DOI 10.17487/RFC8368, May 2018, <https://www.rfc-editor.org/info/rfc8368>.

Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-anima-l2acp-scenarios-00, 2019-02-28:

- *Initial version

draft-carpenter-anima-l2acp-scenarios-01, 2019-10-03:

- *Added discussion of MACsec and WPA2

- *Editorial improvements

draft-carpenter-anima-l2acp-scenarios-02, 2020-04-09:

- *Updated references

- *Editorial improvements

- *Converted to xml2rfc v3

Authors' Addresses

Brian Carpenter
The University of Auckland
School of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Bing Liu
Huawei Technologies
Q14, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing
100095
P.R. China

Email: leo.liubing@huawei.com