sfc
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

R. Maglione
G. Trueba
C. Pignataro
Cisco Systems

October 31, 2016

RADIUS Attributes for NSH
draft-maglione-sfc-nsh-radius-01

Abstract

Network Service Header (NSH) protocol defines the Service Function Chaining (SFC) encapsulation required to support the Service Function Chaining (SFC) Architecture. One of the components of the Network Service Header (NSH) protocol is the Service Path Identifier (SPI), which identifies a service path, another important element of the NSH protocol is the Service Index (SI), which provides location within the Service Path.

When Service Providers would like to deliver customized services offers requiring Service Functions Chains, a different service chain may be required for each subscriber or group of subscribers. In order to simplify the service provisioning in this scenario, it would be useful to be able to associate the Service Path Identifier (SPI), identifying the service chain, and the appropriate Service Index (SI), identifying the location in the service path, with the customer profile.

In some Broadband networks, the customer profile information may be stored in Authentication, Authorization, and Accounting (AAA) servers. This document specifies two new Remote Authentication Dial-In User Service (RADIUS) attributes to carry the Service Path Identifier (SPI) and the Service Index (SI).

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 May 4, 2017.

Table of Contents

1. Introduction

Network Service Header (NSH) protocol [I-D.ietf-sfc-nsh] defines the Service Function Chaining (SFC) encapsulation required to support the Service Function Chaining (SFC) Architecture [RFC7665]. One of the components of the Network Service Header (NSH) protocol is the Service Path Identifier (SPI), which identifies a service path, another important element of the NSH protocol is the Service Index (SI), which provides location within the Service Path.

When Service Providers would like to deliver customized services offers requiring Service Functions Chains, a different service chain may be required for each subscriber or group of subscribers. In order to simplify the service provisioning in this scenario, it would be useful to be able to associate the Service Path Identifier (SPI), identifying the service chain, and the appropriate Service Index (SI) identifying the location in the service path, with the customer profile.

In some Broadband networks, the customer profile information may be stored in Authentication, Authorization, and Accounting (AAA) servers. This document specifies two new Remote Authentication Dial-In User Service (RADIUS) attributes to carry the Service Path Identifier (SPI) and the Service Index (SI).

1.1. Requirements Language

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. Terminology

NSH Network Service Header

SFC Service Function Chaining

SFF Service Function Forwarder

SPI Service Path Identifier

SI Service Index

3. Architectural Model

Figure 1 illustrates the network reference model for a Broadband access scenario where a NAS, acting as RADIUS Client, performs both the Service Classification and Service Forwarder Function.

The Service Functions which make up the Service Chaining are part of the SP network and they are not depicted in Figure 1

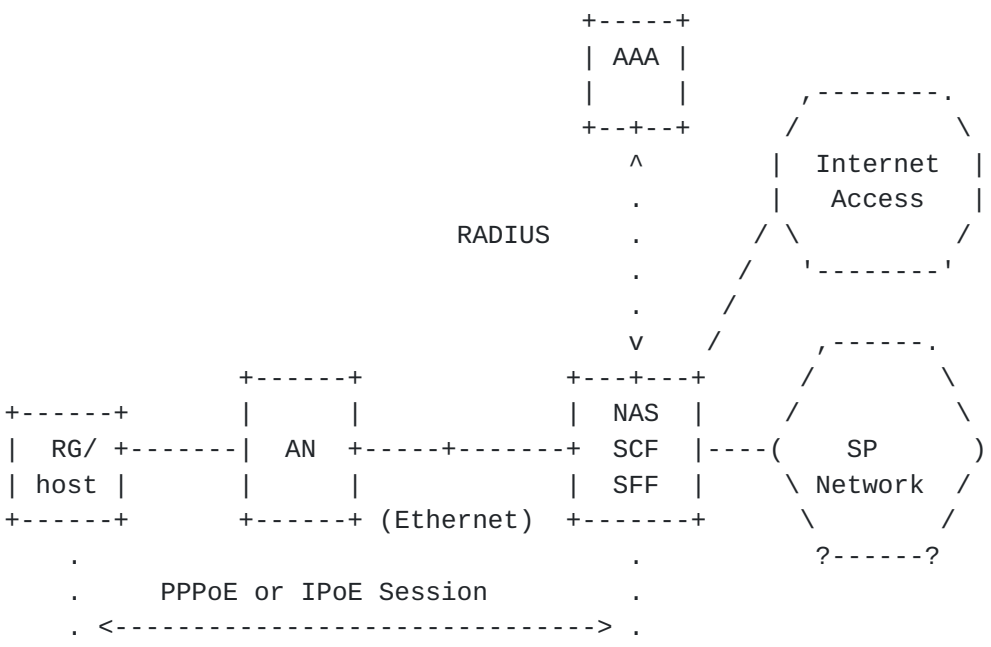

Figure 1: Network Reference Model

Here there is a brief description of the Authentication/Authorization process between the NAS and the AAA Server.

The NAS initially sends a RADIUS Access-Request message to the RADIUS server, requesting authentication. Once the RADIUS server receives the request, it validates the sending client, and if the request is approved, the AAA server replies with an Access-Accept message including a list of attribute-value pairs that describe the parameters to be used for this session. This list MAY also contain the NSH Service Path Identifier (NSH-SPI) and the NSH Service Index (NSH-SI) attributes used to identify a specific service path and the location in the service path.

The NSH SPI attribute returned by AAA Server in the Access-Accept is used by the NAS to insert the traffic of the subscriber in the correct service path. A classification rule, to be associated with the SPI, can also be sent by the AAA Server as part of the list of attribute-value pairs.

4. RADIUS Attributes

This section defines the NSH Service Path Identifier (SPI) and the NSH Service Index (SI) attributes that are used in the above-mentioned scenario. The attributes design follows [RFC6158] and refers to [RFC6929] and [I-D.ietf-radext-datatypes].

4.1. NSH Service Path Identifier

The NSH Service Path Identifier (NSH-SPI) RADIUS attribute contains the value which identifies a specific service path to be associated to a subscriber.

When the NAS receives from the AAA Server the NSH-SPI attribute, the NAS MUST use the value contained in this attribute to populate the Service Path Identifier (SPI) field in the NSH Service Path header defined in [I-D.ietf-sfc-nsh].

If the NAS is pre-configured with a default NSH SPI value, this value MAY be inserted in the attribute. The RADIUS server MAY ignore the hint sent by the NAS, and it MAY assign a different NSH SPI.

If the NAS includes the NSH-SPI attribute, but the AAA server does not recognize it, this attribute MUST be ignored by the AAA server. If the NAS does not receive the NSH-SPI attribute in the Access-Accept message, it MAY fall back to a pre-configured default NSH SPI, if any. If the NAS receives the NSH-SI attribute, but it does not receives the NSH-SPI attribute from the AAA Server and the NAS does not have any pre-configured SPI, the traffic generated by that specific subscriber MUST be dropped as this is an error condition. If the NAS does not receive the NSH-SPI attribute and it does not receive the NSH-SI attribute in the Access-Accept message and the NAS does not have any pre-configured NSH SPI and NSH SI, the traffic generated by that specific subscriber does not have to be sent across any service chain.

If the NAS is pre-provisioned with a default NSH SPI and the NSH-SPI received in the Access-Accept message is different from the configured default, then the NSH-SPI received in the Access-Accept message MUST be used for the session.

If an implementation includes Change-of-Authorization (CoA) messages [RFC5176], they could be used to modify the current specified SPI. When the NAS receives a CoA Request message containing the NSH-SPI attribute, the NAS MUST use the received NSH SPI value to re-configure the the Service Path Identifier (SPI) field in the NSH Service Path header. This allows the network administrator to modify the forwarding of the traffic of a specific subscriber. By changing the SPI value the service path used for the subscriber is modified, thus the traffic of the selected subscriber is sent across a different service chain.

The NSH-SPI RADIUS attribute MUST NOT appear more than once in a message.

A summary of the NSH-SPI RADIUS attribute format is shown below. The fields are transmitted from left to right.

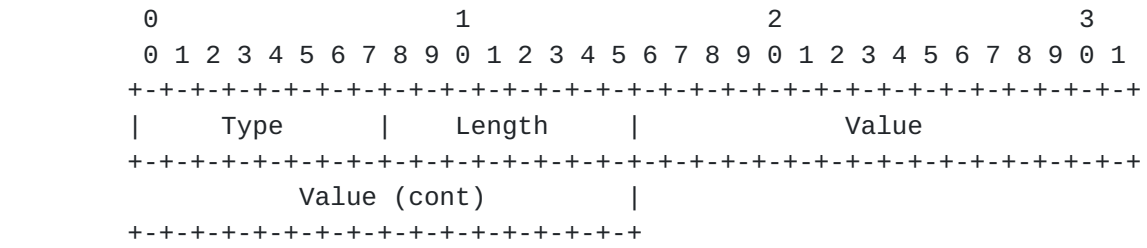

Figure 2: NSH-SPI RADIUS Attribute

Type TBD - NSH-SPI

Length 6

Value This field uses the integer data type, defined in [I-D.ietf-radext-datatypes], which encodes a 32-bit unsigned integer in network byte order. As the Service Path Identifier field, defined in [I-D.ietf-sfc-nsh], is limited to 24 bits, only 24 bits of the value field in the RADIUS attribute are used to encode the NSH-SPI value. The NAS acting as classifier MUST copy this value into the SPI field of the NSH Service Path Header.

4.2. NSH Service Index

The NSH Service Index (NSH-SI) RADIUS attribute contains the value which identifies the location in the service path. According to [I-D.ietf-sfc-nsh] , the initial SI value SHOULD default to 255.

When the NAS receives from the AAA Server the NSH-SI attribute, the NAS MUST use the value contained in this attribute to populate the Service Index (SI) field in the NSH Service Path header defined in [I-D.ietf-sfc-nsh].

If the NAS is pre-configured with a default NSH SI value, this value MAY be inserted in the attribute. The RADIUS server MAY ignore the hint sent by the NAS, and it MAY assign a different NSH SI.

If the NAS includes the NSH-SI attribute, but the AAA server does not recognize it, this attribute MUST be ignored by the AAA server. If the NAS does not receive the NSH-SI attribute in the Access-Accept message, but it receives the NSH-SPI attribute, it MAY fall back to a pre-configured default NSH SI, if any. If the NAS receives the NSH-SPI attribute, but it does not receives the NSH-SI attribute from the AAA Server and the NAS does not have any pre-configured SI, the

traffic generated by that specific subscriber MUST be dropped as this is an error condition.

If the NAS is pre-provisioned with a default NSH SI and the NSH-SI received in the Access-Accept message is different from the configured default, then the NSH-SI received in the Access-Accept message MUST be used for the session.

If an implementation includes Change-of-Authorization (CoA) messages [RFC5176], they could be used to modify the current specified NSH SI. When the NAS receives a CoA Request message containing the NSH-SI attribute, the NAS MUST use the received NSH SI value to re-configure the the Service Index (SI) field in the NSH Service Path header.

The NSH-SI RADIUS attribute MUST NOT appear more than once in a message.

A summary of the NSH-SI RADIUS attribute format is shown below. The fields are transmitted from left to right.

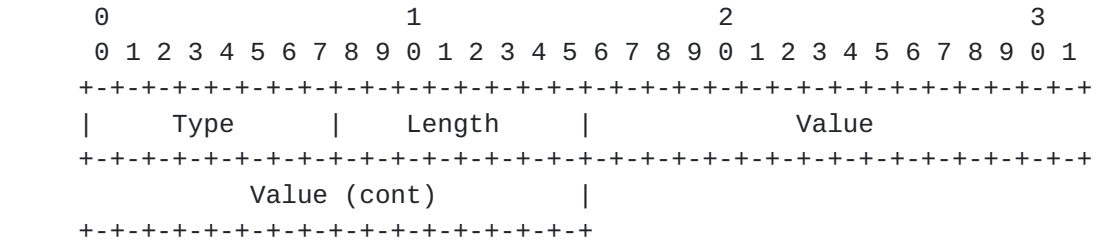

Figure 3: NSH-SI RADIUS Attribute

Type TBD - NSH-SI

Length 6

Value This field uses the integer data type defined in [I-D.ietf-radext-datatypes], which encodes a 32-bit unsigned integer in network byte order. As the Service Index field defined in [I-D.ietf-sfc-nsh] is limited to 8 bits, only 8 bits of the value field in the RADIUS attribute are used to encode the NSH-SI value. The NAS acting as classifier MUST copy this value into the SI field of the NSH Service Path Header.

5. Table of Attributes

The following tables provide a guide to which attributes may be found in which kinds of packets, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Challenge	Accounting-Request	#	Attribute
0-1	0-1	0	0	0-1	TBD	NSH-SPI
0-1	0-1	0	0	0-1	TBD	NSH-SI

CoA-Request	CoA-ACK	CoA-NACK	#	Attribute
0-1	0	0	TBD	NSH-SPI
0-1	0	0	TBD	NSH-SI

The following table defines the meaning of the above table entries.

0 This attribute MUST NOT be present in the packet.

0+ Zero or more instances of this attribute MAY be present in the packet.

0-1 0-1 Zero or one instance of this attribute MAY be present in the packet.

6. Diameter Considerations

These attributes are usable within either RADIUS or Diameter [RFC6733]. Since the attributes defined in this document have been allocated from the standard RADIUS type space, no special handling is required by Diameter entities.

7. Acknowledgements

The authors would like to thank Jim Guichard and Mohamed Boucadair for their valuable comments and inputs to this document.

8. IANA Considerations

Per this document, IANA is requested to assign two new RADIUS Attribute Type in the "Radius Types" registry (currently located at http://www.iana.org/assignments/radius-types) for the following attributes:

TBD NSH-SPI integer

TBD NSH-SI integer

9. Security Considerations

This document has no additional security considerations beyond those already identified in [RFC2865] for the RADIUS protocol and in [RFC5176] for CoA messages.

The security considerations for NSH protocol are described in section 9 of [I-D.ietf-sfc-nsh]

10. References

10.1. Informative References

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, DOI 10.17487/RFC5176, January 2008, <http://www.rfc-editor.org/info/rfc5176>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <http://www.rfc-editor.org/info/rfc7665>.

10.2. Normative References

[I-D.ietf-radext-datatypes] DeKok, A., "Data Types in the Remote Authentication Dial-In User Service Protocol (RADIUS)", draft-ietf-radext-datatypes-08 (work in progress), October 2016.

[I-D.ietf-sfc-nsh] Quinn, P. and U. Elzur, "Network Service Header", draft-ietf-sfc-nsh-10 (work in progress), September 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.

[RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <http://www.rfc-editor.org/info/rfc6158>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, DOI 10.17487/RFC6929, April 2013, <http://www.rfc-editor.org/info/rfc6929>.

Authors' Addresses

Roberta Maglione
Cisco Systems
Via Torri Bianche 8
Vimercate
Italy

Email: robmgl@cisco.com

Guillermo Trueba
Cisco Systems
Avenida Cortes Valencianas 58
Valencia 46015
Spain

Email: gtrueba@cisco.com

Carlos Pignataro
Cisco Systems
7200 Kit Creek Road
Research Triangle Park, NC 27709
USA

Email: cpignata@cisco.com