Network Working Group
Internet-Draft
Expires: February 16, 2005

R. Droms
J. Schnizlein
Cisco Systems
August 18, 2004

RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option
draft-ietf-dhc-agentopt-radius-08.txt

Abstract

A NAS (network access server) may choose to authenticate the identity of a device before granting that device access to the network. The IEEE 802.1X protocol is an example of a mechanism for providing authenticated layer 2 network access. A network element using RADIUS as an authentication authority will receive attributes from a RADIUS server that may be used by a DHCP server in the selection of configuration parameters to be delivered to the device through its DHCP client. The RADIUS Attributes sub-option enables a network element to pass along attributes for the user of a device received

during RADIUS authentication to a DHCP server.

1. Introduction and Background

The RADIUS Attributes sub-option for the DHCP Relay Agent option provides a way in which a NAS can pass attributes obtained from a RADIUS server to a DHCP server [1]. IEEE 802.1X [2] is an example of a mechanism through which a NAS such as a switch or a wireless LAN access point can authenticate the identity of the user of a device before providing layer 2 network access using RADIUS as the Authentication Service specified in RFC3580 [10]. In IEEE 802.1X authenticated access, a device must first exchange some authentication credentials with the NAS. The NAS then supplies these credentials to a RADIUS server, which eventually sends either an Access-Accept or an Access-Reject in response to an Access-Request. The NAS, based on the reply of the RADIUS server, then allows or denies network access to the requesting device.

Figure 1 summarizes the message exchange among the participants in IEEE 802.1X authentication.

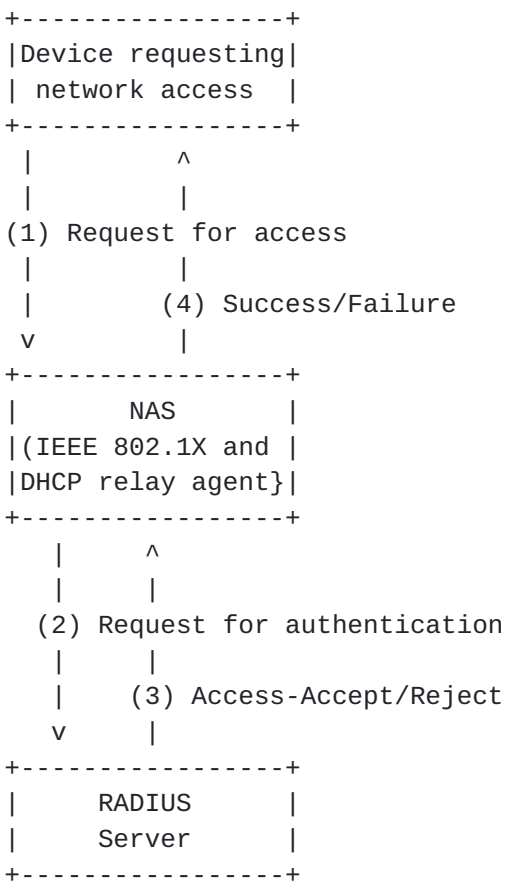


Figure 1

In the application described in this document, the access device acts as an IEEE 802.1X Authenticator and adds a DHCP relay agent option which includes a RADIUS Attributes sub-option to DHCP messages. At the successful conclusion of IEEE 802.1X authentication, a RADIUS Access-Accept provides attributes for service authorizations to the NAS. The NAS stores these attributes locally. When the NAS subsequently forwards DHCP messages from the network device, the NAS adds these attributes in a RADIUS Attributes sub-option. The RADIUS Attributes sub-option is another suboption of the Relay Agent Information option [5].

This document uses IEEE 802.1X as an example to motivate the use of RADIUS by a NAS. The RADIUS Attributes sub-option described in this document is not limited to use in conjunction with IEEE 802.1X and can be used to carry RADIUS attributes obtained by the relay agent for any reason. That is, the option is not limited to use with IEEE 802.1X, but is constrained by RADIUS semantics (see Section 4).

The scope of applicability of this specification is such that robust interoperability is only guaranteed for RADIUS service implementations that exist within the same scope as the DHCP service implementation, i.e. within a single, localized administrative domain. Global interoperability of this specification, across administrative domains, is not required.

2. Terminology

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 RFC 2119 [3].

The use of the standard keywords MUST, SHOULD, MUST NOT and SHOULD NOT within this specification are with respect to RADIUS clients and servers that implement the optional features of this specification, do not create any normative requirements outside of that scope and do not modify the base RADIUS specifications, such as RFC2865 or RFC2866.

2.1 DHCP Terminology

The following terms are used as defined in RFC2131 and RFC3046: DHCP relay agent, DHCP server, DHCP client.

2.2 RADIUS Terminology

The following terms are used in conjunction with RADIUS:

RADIUS server: A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Attribute: A Type-Length-Value tuple encapsulating data elements as defined in RFC 2865 [4].

NAS: A Network Access Server (NAS) provides access to the network and operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned. Unlike a traditional dial NAS, the NAS considered here may not have a protocol like PPP through which it can pass configuration information from the RADIUS attributes to the client

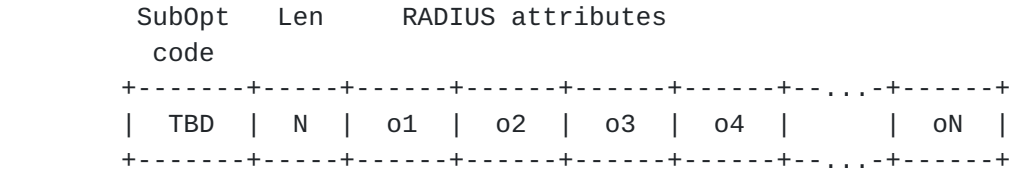
2.3 IEEE 802.1X Terminology

The following terms are used as defined in the IEEE 802.1X protocol: Authenticator, Supplicant.

3. RADIUS Attributes sub-option format

The RADIUS Attributes Sub-option is a new sub-option for the DHCP Relay Agent option.

The format of the RADIUS Attributes sub-option is:



The RADIUS attributes are encoded according to the encoding rules in RFC 2865, in octets o1...oN.

The DHCP relay agent truncates the RADIUS attributes to fit in the RADIUS Attributes sub-option.

4. DHCP Relay Agent Behavior

When the DHCP relay agent receives a DHCP message from the client, it MAY append a DHCP Relay Agent Information option containing the RADIUS Attributes sub-option, along with any other sub-options it is configured to supply. The RADIUS Attributes sub-option MUST only contain the attributes provided in the RADIUS Access/Accept message. The DHCP relay agent MUST NOT add more than one RADIUS Attributes sub-option in a message.

The relay agent MUST include the User-Name and Framed-Pool attributes in the RADIUS Attributes sub-option if available, and MAY include other attributes.

To avoid dependencies between the address allocation and other state information between the RADIUS server and the DHCP server, the DHCP relay agent SHOULD include only the attributes in the table below an instance of the RADIUS Attributes sub-option. The table, based on the analysis in RFC 3580 [10], lists attributes that MAY be included:

#	Attribute
1	User-Name (RFC 2865 [3])
6	Service-Type (RFC 2865)
26	Vendor-Specific (RFC 2865)
27	Session-Timeout (RFC 2865)
88	Framed-Pool (RFC 2869)
100	Framed-IPv6-Pool (RFC 3162 [8])

5. DHCP Server Behavior

When the DHCP server receives a message from a relay agent containing a RADIUS Attributes sub-option, it extracts the contents of the sub-option and uses that information in selecting configuration parameters for the client. If the relay agent forwards RADIUS attributes not included in the table in Section 4, the DHCP server SHOULD ignore them. If the DHCP server uses attributes not specified here, it might result in side effects not anticipated in the existing RADIUS specifications.

6. DHCP Client Behavior

Relay agent options are exchanged only between relay agents and DHCP server, so DHCP clients are never aware of their use.

7. Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in RFC 3118 [8]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in RFC 2131 [1].

The DHCP Relay Agent option depends on a trusted relationship between the DHCP relay agent and the server, as described in section 5 of RFC 3046 [5]. While the introduction of fraudulent relay-agent options can be prevented by a perimeter defense that blocks these options unless the relay agent is trusted, a deeper defense using the

authentication option for relay agent options [11] or IPsec [12] SHOULD be deployed as well.

8. IANA Considerations

IANA has assigned the value of TBD for the DHCP Relay Agent Information option sub-option code for this sub-option. This document does not define any new namespaces or other constants for which IANA must maintain a registry.

9. Acknowledgments

Expert advice from Bernard Aboba, Paul Funk, David Nelson, Ashwin Palekar and Greg Weber on avoiding RADIUS entanglements is gratefully acknowledged.

Normative References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[2] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port based Network Access Control", IEEE Standard 802.1X, March 2001.

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

[4] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

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

Informative References

[6] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[7] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[8] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[9] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[10] Congdon, P., Aboba, B., Smith, A., Zorn, G. and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[11] Stapp, M. and T. Lemon, "The Authentication Suboption for the DHCP Relay Agent Option", draft-ietf-dhc-auth-suboption-02 (work in progress), October 2003.

[12] Droms, R., "Authentication of DHCP Relay Agent Options Using IPsec", draft-ietf-dhc-relay-agent-ipsec-00 (work in progress), September 2003.

Authors' Addresses

Ralph Droms
Cisco Systems
1414 Massachusetts Avenue
Boxborough, MA 01719
USA

EMail: rdroms@cisco.com

John Schnizlein
Cisco Systems
9123 Loughran Road
Fort Washington, MD 20744
USA

EMail: jschnizl@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.